baramundi

Release Notes

baramundi Management Suite

2024 R1

Empower your IT

Liebe Leser:innen,

Dieses Release bietet neue Features und eine Vielzahl von Usability-Optimierungen, um die Nutzung der bMS sowohl für IT-Admins als auch für Endbenutzer:innen zu verbessern.

Viele der Features tragen zu noch mehr Sicherheit in der IT bei:

- Dies betrifft im Kontext von **Defense Control** auf Administrationsseite die optimale Nutzung von **Passwörtern**, um Angriffsvektoren zu verringern.
- Für **Mobilgeräte** besteht auch in Zeiten von Cloud-Speichern weiterhin der Bedarf, sicher auf On-Premises-Unternehmensdaten zugreifen zu können. Hierfür ist das neue, verwaltbare **Per-App VPN** nützlich, wodurch zwischen einzelnen Business-Apps und dem Unternehmen sichere Tunnelverbindungen nutzbar werden.

Bei der Optimierung der End-User-Experience hilft das Einholen von quantitativem und qualitativem **Nutzerfeedback** über **Argus Experience**. Dank graphischer Statistiken können Admins so einfach Handlungsempfehlungen ableiten und etwaigen Tickets zuvorkommen.

Darüber hinaus gibt es Detailverbesserungen für Universelle Dynamische Gruppen, Geräteidentifikation per UUID, Linux-Inventarisierung, Android-Management und unserer Schnittstelle bConnect.

Ich wünsche Ihnen eine anregende Lektüre.

Armin Leinfelder

Director Product Management

baramundi Management Suite – Version 2024 R1

INHALTSVERZEICHNIS

1 Release 2024 R1

1.1 Defense Control

1.1.1 Verwaltung des lokalen Administratorenpassworts

Bei der Härtung von IT-Umgebungen gehört auch dazu, dass die User an ihren Geräten nur eingeschränkte und insbesondere keine administrativen Berechtigungen besitzen. Dennoch kann es in Einzelfällen erforderlich sein, sich am Gerät als lokaler Admin anzumelden. Ein pauschales Deaktivieren des lokalen Administratorenkontos erschwert im Zweifel die Problemsuche und -lösung. Dennoch sollte der lokale Administrator nicht überall dasselbe Kennwort besitzen, denn auch das schwächt die Sicherheit fundamental.

Lokaler Admin, aber sicher!

Um die Geräte nun bestmöglich abzusichern und dennoch einen administrativen Zugang zu erhalten, auch wenn z. B. keine Netzwerkverbindung besteht, kann die bMS ein lokales Administratorenkonto auf den Endpoints verwalten. Hierzu werden zunächst die Rahmenbedingungen wie der Benutzername des lokalen Admins (auch mit Variablen), die Länge des Passworts und die Gültigkeitsdauer festgelegt. Anschließend verwaltet die bMS die Konten auf den Endpoints und kümmert sich um die zyklische Neugenerierung der Passwörter.

Abbildung 1 – Konfiguration für die Anlage eines, durch die bMS verwalteten, lokalen Administrators

Die Passwörter können über das baramundi Management Center eingesehen und z. B. an einen Techniker vor Ort weitergegeben werden. Selbstverständlich kann das Passwort nach Herausgabe umgehend zurückgesetzt bzw. neu generiert werden.

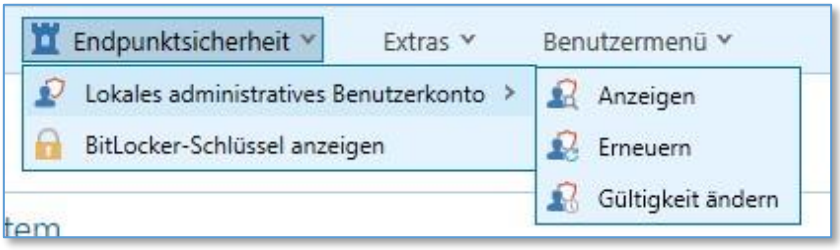


Abbildung 2 – Neues Kontextmenü „Endpunktsicherheit"

Die dynamischen Anmeldedaten für den durch die bMS verwalteten Administrations-Account sind auch als Variable im bMC zur Verwendung verfügbar, z. B. in „Benutzerdefinierte Clientbefehle“.

1.2 Mobile Devices

1.2.1 Sicherer Zugriff auf Unternehmensdaten für Apps (Per-App VPN)

Das mobile Arbeiten ist das neue „Normal“ und ist ein fester Bestandteil der modernen Arbeitswelt geworden. Um fernab des Unternehmensnetzes aber wirklich produktiv arbeiten zu können, ist ein sicherer Zugriff auf Unternehmensdaten unabdingbar. Zahlreiche Daten und Services liegen bereits in der Cloud und sind somit jederzeit und von jedem berechtigten Gerät abrufbar – aber was ist mit den Daten und Services, die noch nicht in der Cloud verfügbar sind oder auch ganz bewusst nicht dort abgelegt werden sollen?

Diese Daten bleiben im Unternehmensnetz und sind von der Außenwelt abgeschottet. Der einzige Weg ins Unternehmensnetz führt über ein Virtuelles Privates Netzwerk, kurz VPN. Schon seit Jahren ist es möglich, mit der bMS ein VPN auf mobilen Geräten einzurichten. So können sich die mobilen Geräte ins Unternehmensnetz verbinden und die Apps auf die dortigen Ressourcen zugreifen. Doch diese gesicherte Verbindung findet stets systemweit statt und so haben alle Apps Zugriff auf das Unternehmensnetz – neben der gewünschten App für das ERP erlangt so auch der private Messenger Zugriff. Gerade in einer Zeit, in der die private Nutzung der Unternehmensgeräte zunimmt, ist auch hier eine klare Trennung zwischen privaten und Unternehmenszwecken absolut notwendig.

1.2.1.1 Konzept

Die Antwort ist simpel: Das VPN wird nur für einzelne Apps aufgebaut. Ist eine App autorisiert, wird der Netzwerkverkehr der App sicher verschlüsselt über das VPN ins Unternehmensnetz geleitet.

Normalerweise ist für diesen Fall eine komplexe Konfiguration im internen Netz und auch am Endgerät nötig – diese Komplexität wird komplett durch die bMS behandelt.

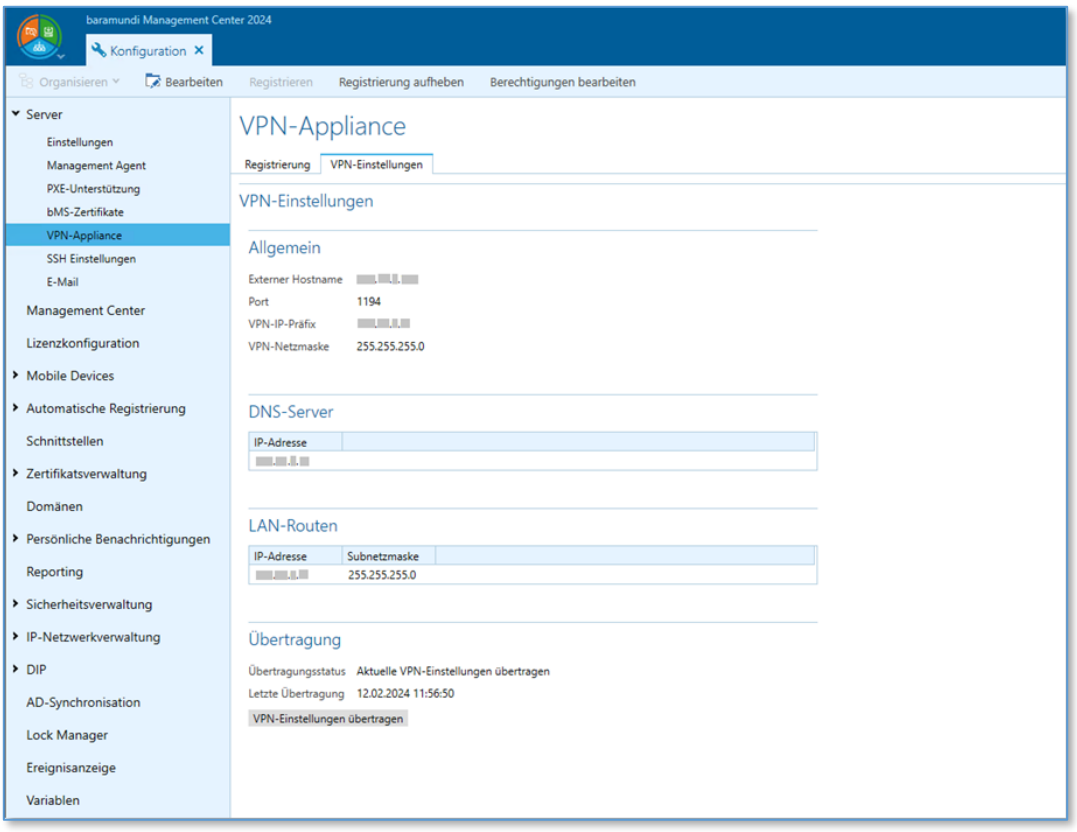


Abbildung 3 – Konfigurationsseite für die Einstellungen der VPN-Appliance

Die Lösung besteht aus einer App auf dem Endgerät (iOS/Android) und einer virtuellen Appliance in der DMZ (demilitarisierte Zone). Nach der Ersteinrichtung der Appliance wird diese komplett durch die bMS verwaltet. Die Zugänge über das VPN werden per Clientzertifikat abgesichert – nur gültige, von der bMS ausgestellte Zertifikate werden akzeptiert.

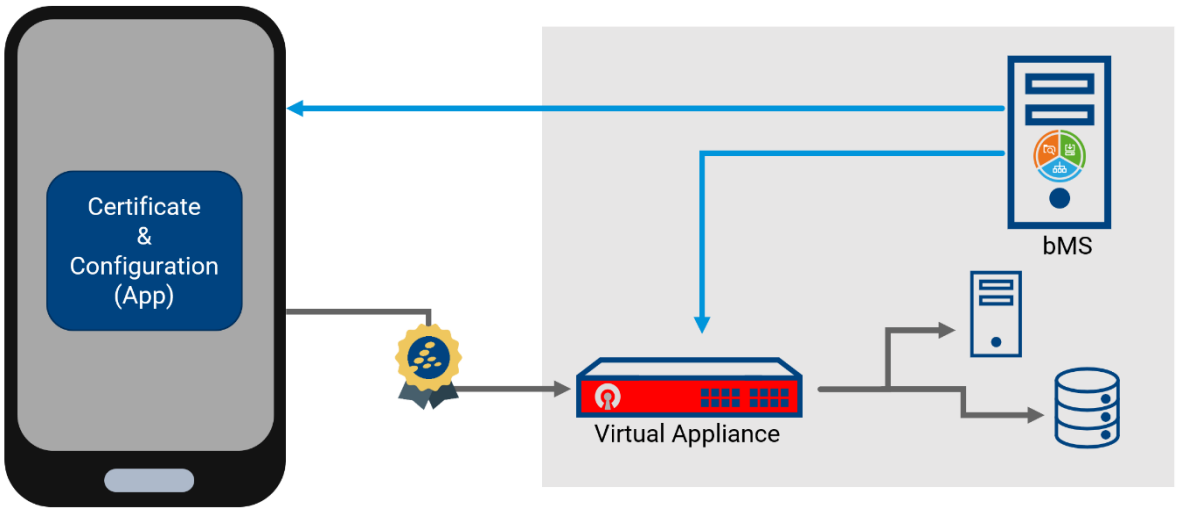


Abbildung 4 – Schematische Darstellung des Ablaufs bei der VPN-Einrichtung

1.2.1.2 Handhabung durch die Admins

Um den Zugriff für einzelne Apps auf einem Gerät freizugeben, muss zuerst eine VPN-App auf dem jeweiligen Gerät installiert und konfiguriert werden – diese ermöglicht es dem Gerät, eine Verbindung zur baramundi-VPN-Appliance herzustellen und sich zu authentifizieren. Beides passiert im Rahmen eines Jobs.

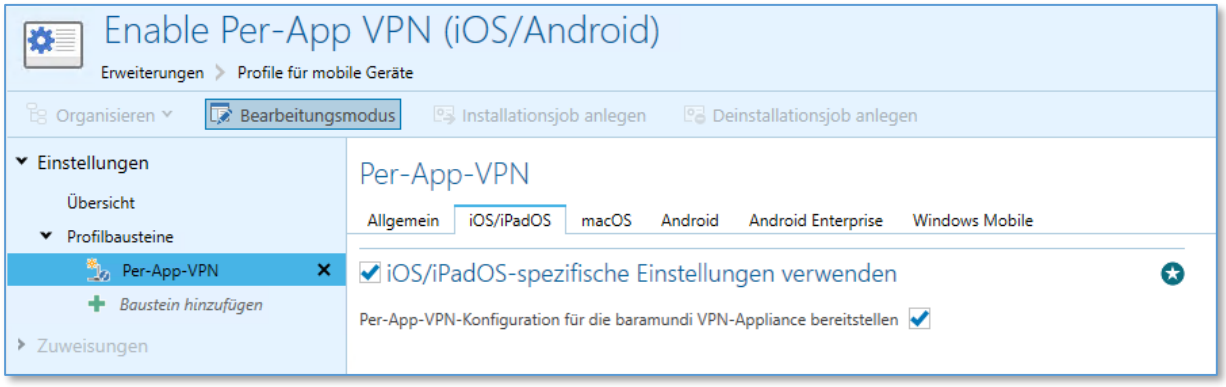


Abbildung 5 – Aktivierung der VPN-Funktion per Profilbaustein

Selbstverständlich kann der Zugang via VPN auch per Job aus der Ferne wieder entzogen werden. Hierbei wird das Zertifikat des Geräts vom Gerät entfernt und auf der Appliance gesperrt – auch mit einem eventuell abhandengekommenen Zertifikat kann keine Verbindung mehr aufgebaut werden.

Sobald der grundlegende Zugang eingerichtet ist, können die Unternehmens-Apps für die Verwendung des Per-App-VPN konfiguriert werden. Hierbei muss lediglich im Jobschritt zur Installation der App die Nutzung des VPN aktiviert werden.

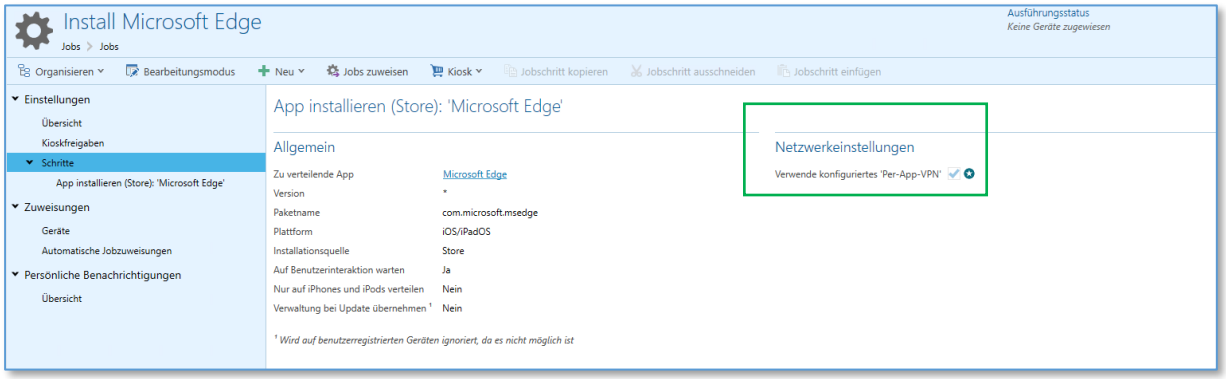


Abbildung 6 – Aktivierung der VPN-Funktion bei der App-Installation

1.2.1.3 Verwendung durch die User

Für die User der Geräte ist die Nutzung des VPN komplett transparent – es sind keine besonderen Aktionen notwendig. Das System kümmert sich selbstständig um den Aufbau des VPN-Tunnels beim Verwenden der berechtigten Unternehmens-Apps.

1.2.1.3.1 Apple iOS

Unter iOS ist der Status der Verbindung in den „Einstellungen“ ersichtlich. Dort kann auch eingesehen werden, welche Apps auf dem Gerät für die Verwendung des VPN eingerichtet sind.

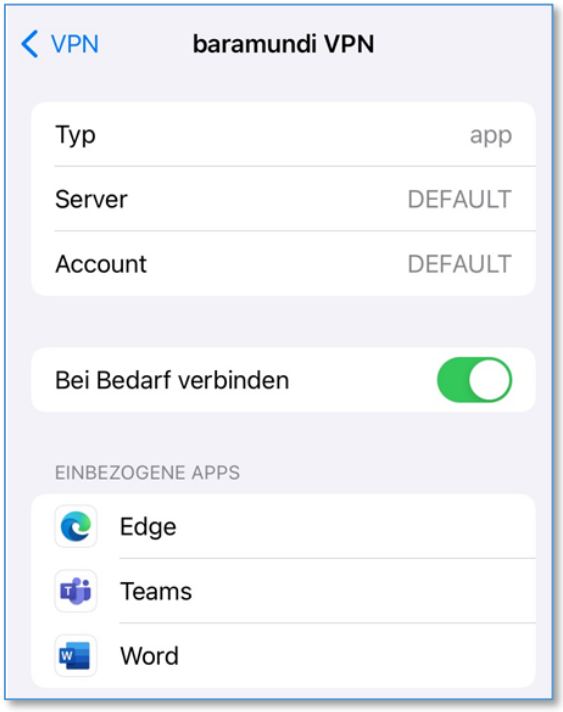


Abbildung 7 – VPN-Einstellungen mit konfiguriertem Per-App-VPN unter iOS

1.2.1.3.2 Google Android

Unter Android ist der Status der Verbindung in der App „baramundi VPN“ ersichtlich.

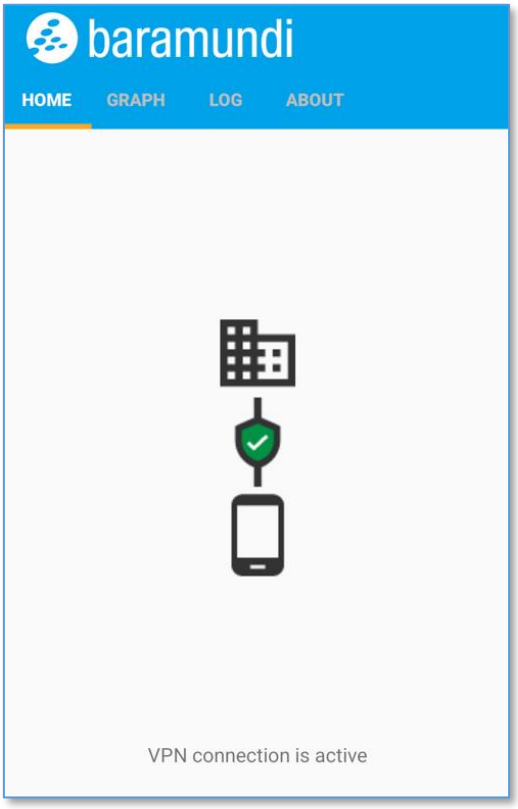


Abbildung 8 – Statusseite der baramundi VPN-App für Android mit verbundenem VPN

1.2.2 Weitere Verbesserungen

1.2.2.1 Unterstützung von WPA3

Der Wifi-Baustein unterstützt die Konfiguration von WP3 Personal und Enterprise auf Apple iOS, Apple macOS und Google Android.

WPA3 Personal	WPA3 Enterprise
ab iOS 13	ab iOS 13
ab macOS 10.15	ab macOS 10.15
ab Android 11	ab Android 12

1.2.2.2 Android

1.2.2.2.1 Neuer Push-Service für Jobverarbeitung

Ab der bMS 2024 werden alle für die Verwaltung von Android-Geräten benötigten Push-Nachrichten über die zentrale baramundi-Infrastruktur versendet. Somit ist keine lokale Konfiguration der Android-Push-Dienste (Firebase Cloud Messaging/FCM) mehr nötig.

Hinweis[1]: *Ab dem 20.06.2024 wird der Push mit älteren bMS bis einschl. 2023 R2 nicht mehr funktionieren – die Geräte arbeiten dann nur noch per zyklischem Abruf der Jobs. Um eine nahtlose Jobverarbeitung per Push zu gewährleisten, sollte vor dem Stichtag auf die aktuelle bMS 2024 aktualisiert werden.*

1.2.2.2.2 WLAN-Konfiguration im Enrollment-Code

Beim Enrollment von Android-Geräten per QR-Code kann nun auch eine Wifi-Konfiguration mitgegeben werden.

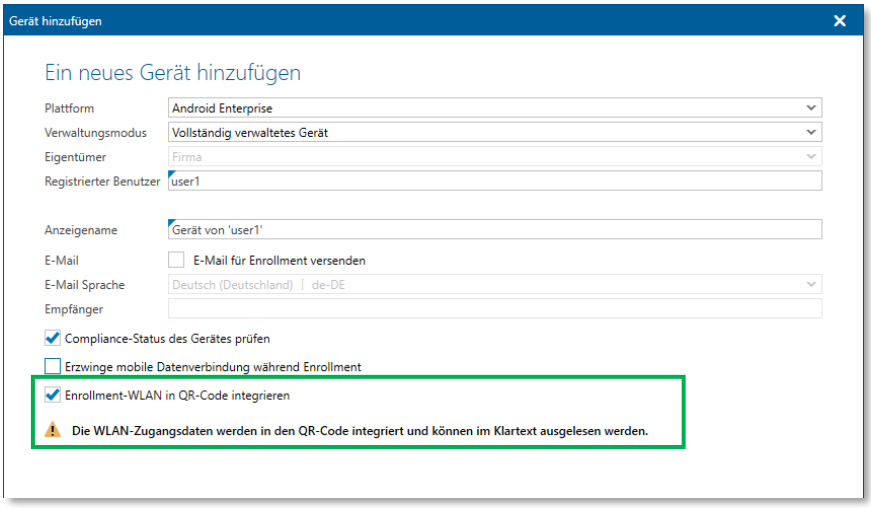


Abbildung 9 – Enrollment-Dialog mit Option für Wifi-Konfiguration und dazugehörigem Hinweis

So muss vor dem Enrollment keine manuelle Verbindung hergestellt werden, der Enrollment-Vorgang wird einfacher und unkomplizierter.

1.2.2.2.3 Entwickleroptionen aktivieren

Über den Baustein „Einschränkungen“ können nun die Entwickleroptionen gesteuert werden. So kann den Usern Zugriff auf z. B. die Debug-Optionen gewährt werden, um auszuwählen, welchen Modus („Nur laden“, „Datenübertragung“, „Android Auto“ etc.) das Gerät beim Verbinden eines USB-Kabels verwenden soll.

Hinweis: *Das Aktivieren der Entwickleroptionen sollte nur so kurz wie möglich erfolgen und nicht auf produktiven Geräten verwendet werden, da aktive Entwickleroptionen die Sicherheit des Geräts herabsetzen – viele Schutzmaßnahmen des Betriebssystems können so umgangen werden!*

[1] https://forum.baramundi.com/index.php?threads/16099/

1.2.2.3 iOS

1.2.2.3.1 Zeitzone setzen

Mit dem neuen Jobschritt „Befehl ausführen“ kann nun die Zeitzone des Geräts definiert werden. Dies ist insbesondere dann erforderlich, wenn die Ortungsdienste am Gerät deaktiviert wurden und somit keine automatische Ermittlung der Zeitzone möglich ist.

1.3 Weiterentwicklungen in Argus Experience

1.3.1 Erfassung von End-User-Feedback

Mit diesem Release ist mit der Erfassung des End-User-Feedbacks ein weiterer wichtiger Meilenstein in baramundi Argus Experience umgesetzt worden. IT-Admins haben damit die Möglichkeit nicht mehr nur auffällige Gerätedaten zu analysieren, sondern auch Rückmeldungen der Mitarbeiter zu deren IT-Umgebung kontinuierlich abzufragen. Das schafft einen ganzheitlichen Blick auf die Arbeitsumgebungen und ermöglicht es dem IT-Admin proaktiv und zielgerichteter mögliche Störfälle zu analysieren.

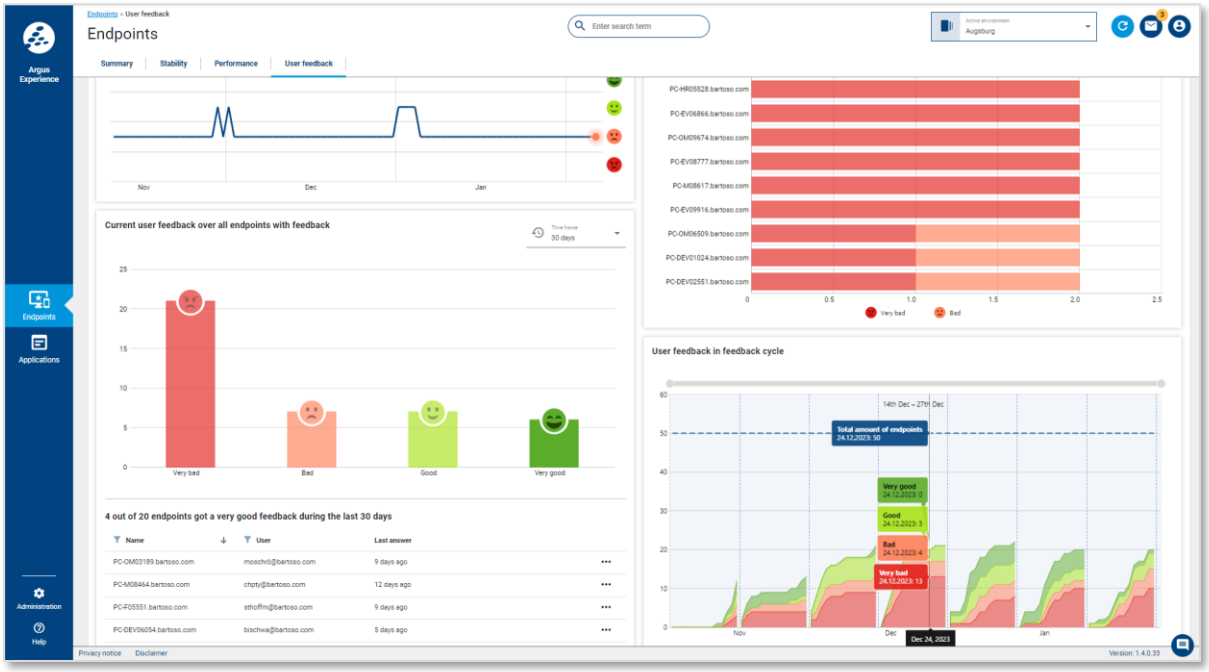


Abbildung 10 – Übersicht von gesammeltem Benutzer-Feedback

1.3.1.1 „Versteckter" Handlungsbedarf durch End-User-Feedback

Man könnte natürlich sagen, dass Admins bereits durch End-User-Tickets ausreichend Rückmeldung von ihren End Usern bekommen. Allerdings ist dieses Feedback meist erst nach einem Störfall entstanden und daher tendenziell negativ. Zielführender ist es, mehr Feedback kontinuierlich und ohne großen Aufwand für den User erfassen zu können.

In folgenden Beispielkonstellationen sind die Rückmeldungen der End User für den IT-Admin sehr hilfreich:

- viele Applikationsabstürze + negatives Feedback
  → **akuter Handlungsbedarf**
- viele Applikationsabstürze + positives Feedback
  → **kein akuter Handlungsbedarf**
- wenig Applikationsabstürze + negatives Feedback
  → **akuter Handlungsbedarf**

Während bei Punkt 1 der akute Handlungsbedarf für den Admin durch das End-User-Feedback eher unterstrichen wird, ändert sich der Handlungsbedarf durch das End-User-Feedback hingegen bei Punkt 2 und 3.

Hätte sich der IT-Admin hier nur auf die Daten der Endgeräte verlassen, hätte er u. U. unnötig eingegriffen (da die Abstürze z. B. nur im Hintergrund stattfanden und die Mitarbeiter nicht in der Arbeit beeinträchtigten) oder zu spät agiert, obwohl die wenigen Abstürze großen Frust und Produktivitätseinbußen der Mitarbeiter nach sich zogen.

In Argus Experience kann der IT-Admin die Umfragezyklen individuell für seine Umgebung konfigurieren und auswerten.

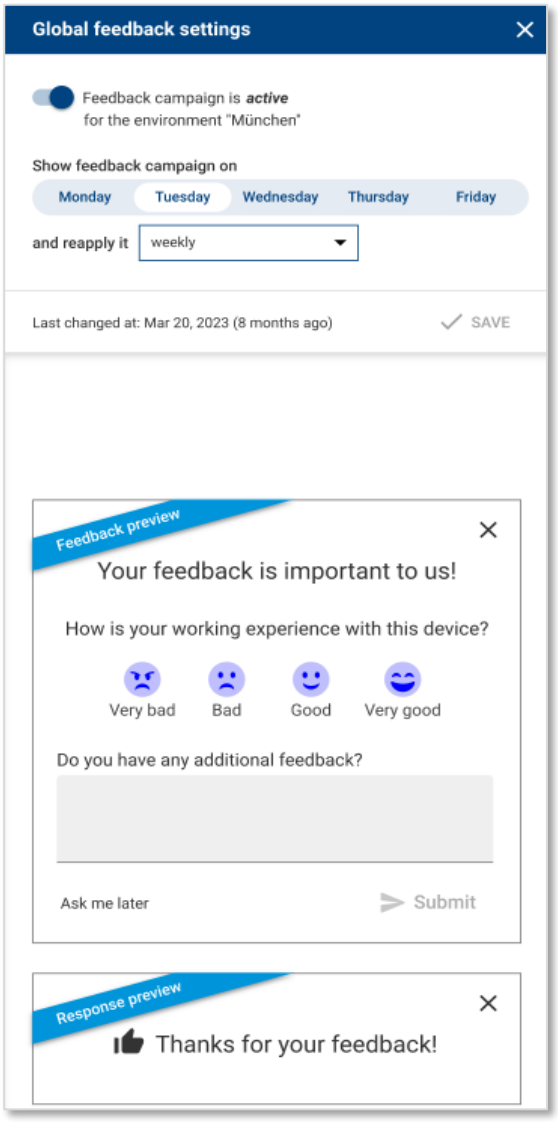


Abbildung 11 – Konfiguration der End-User-Umfragen

1.3.1.2 Detaillierte Rückmeldungen einsehen

Die positive oder negative Rückmeldung der End User ist bereits hilfreich, aber noch nicht ausreichend. Natürlich ist auch der Inhalt des Feedbacks wichtig, um für den IT-Admin besser den Handlungsbedarf ableiten zu können. Mitarbeiter, die sich z. B. kontinuierlich über eine bestimmte Software „beschweren“, können von der IT-Administration proaktiv angesprochen werden und diese kann die Software ggf. aktualisieren, eine Schulung anbieten oder eine alternative Softwarelösung vorschlagen – *bevor* die User mit Tickets eskalieren.

In Argus Experience wird dieses End-User-Feedback übersichtlich auf den Detailseiten der Endgeräte angezeigt.

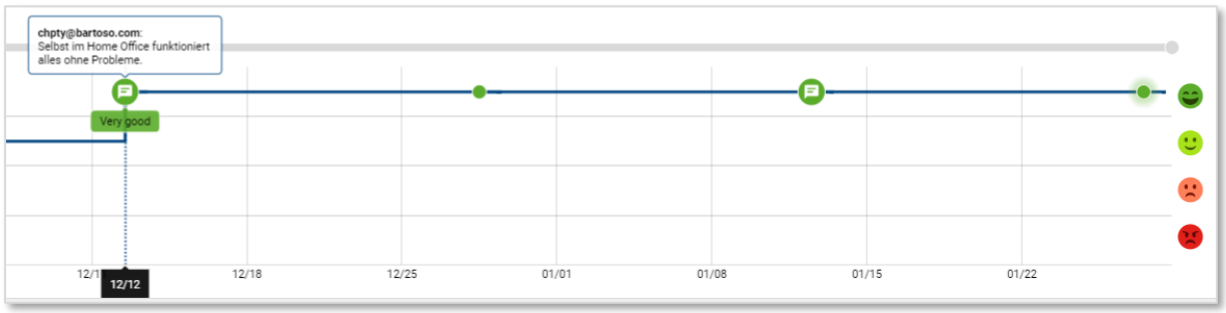


Abbildung 12 – Feedback-Details in Argus Experience

1.3.1.3 Umfragezyklen vergleichen

Wie bereits erwähnt, sollte das Feedback der End User nicht einmalig erfasst werden, sondern kontinuierlich. Das ermöglicht den IT-Admins Veränderungen im IT-Betrieb frühzeitig zu erkennen.

Mit der übersichtlichen Darstellung der Umfragezyklen können die Auswirkungen durchgeführter IT-Maßnahmen analysiert und verglichen werden. So kann z. B. bei einem Umfragezyklus nach einem Windows-11-Rollout analysiert werden, ob die Mitarbeiter mit dem neuen Betriebssystem gut arbeiten können oder ob es noch Probleme in der Benutzung gibt. Ebenso könnten Update-Wellen verschiedener Software mit Umfragezyklen synchronisiert werden, sodass die IT-Administration nicht nur weiß, dass die Umgebung aktuell und sicher ist, sondern dass die User auch angenehm und produktiv arbeiten können.

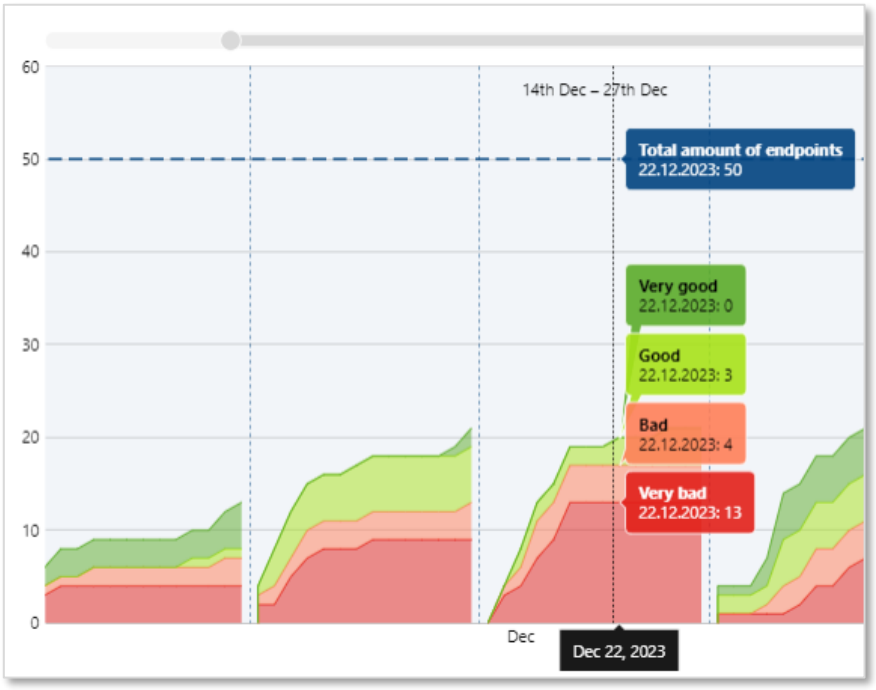


Abbildung 13 – Umfragezyklen vergleichen

1.3.2 Erfassung weiterer Frustquellen

Aber auch weitere Indikatoren werden in Argus Experience erfasst, die potenziell zu großem Frust und/oder zu mangelnder Produktivität der Mitarbeiter führen könnten. Folgende weitere Indikatoren können in Zukunft[2] in Argus Experience erfasst und analysiert werden:

- **Bluescreens**

  Wenn nicht nur eine Applikation abstürzt, sondern gleich der ganze Rechner, dann sorgt das bei den Mitarbeitenden für großen Frust. Schwierig war dabei oft die anschließende Fehleranalyse für den IT-Admin. Die Erkennung und Fehleranalyse in Argus Experience wird „Licht ins Dunkel“ für diese Frustquellen bringen.
- **CPU- und Arbeitsspeicherauslastung**

  Eine Reihe von Rechnern im Unternehmen ist entweder sehr stark ausgelastet oder „dreht Däumchen“. Um den Beschaffungsprozess für neue Computer besser an der zu erwartenden Nutzung und Auslastung zu orientieren, werden auffällige Auslastungen in Argus Experience sichtbar gemacht.
- **Applikationsbasierte Bootzeit**

  Es ist bereits erkennbar, welche Endgeräte sehr lange Startzeiten haben. Bisher war es aber nicht ersichtlich, welche Applikationen diese langen Startzeiten verursachen. Diese Granularität der Bootzeit auf Applikationsebene wird in Argus Experience erweitert, sodass langsame Applikationen von der IT-Administration proaktiv aktualisiert oder ersetzt werden können.

[2] Durch die kontinuierlichen Releases von Argus Experience ist es möglich, dass einige Umsetzungen erst nach Redaktionsschluss dieses Dokuments veröffentlicht werden. Release-Updates hier: https://www.baramundi.com/de-de/management-suite/module/argus-experience/updates

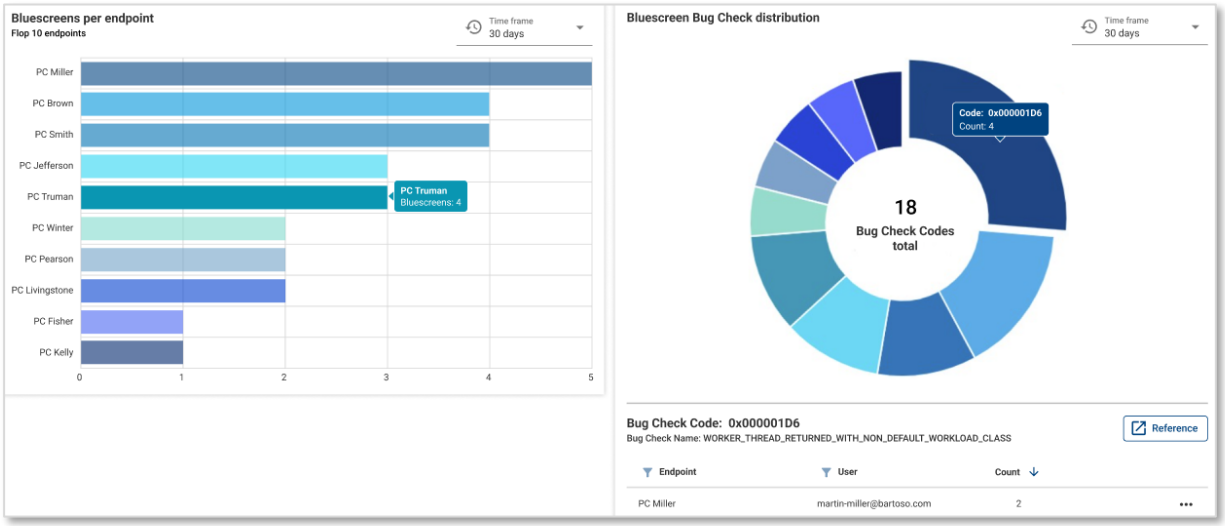


Abbildung 14 – UI-Prototyp „Erfassung weiterer Frustquellen“

1.4 Weitere Verbesserungen

1.4.1 Neue Kriterien für Universelle Dynamische Gruppen

Seit Einführung unserer Universellen Dynamischen Gruppen werden diese stetig erweitert. Nach Einführung der „Automatischen Zuweisung“ von Jobs auf UDGs haben wir diese mit dem neuen Release noch anpassbarer gestaltet.

Mit drei neuen Bedingungen lassen sich noch granularer Gruppen bilden. Diese können mit allen UDG-Features versehen werden, wie bspw. mit dem Sync nach Argus Cockpit oder auch den eben genannten automatischen Zuweisungen.

1.4.1.1 Software

Die Universellen Dynamischen Gruppen erhalten mit dem Release eine neue Bedingung für installierte Software auf dem entsprechenden Endpunkt.

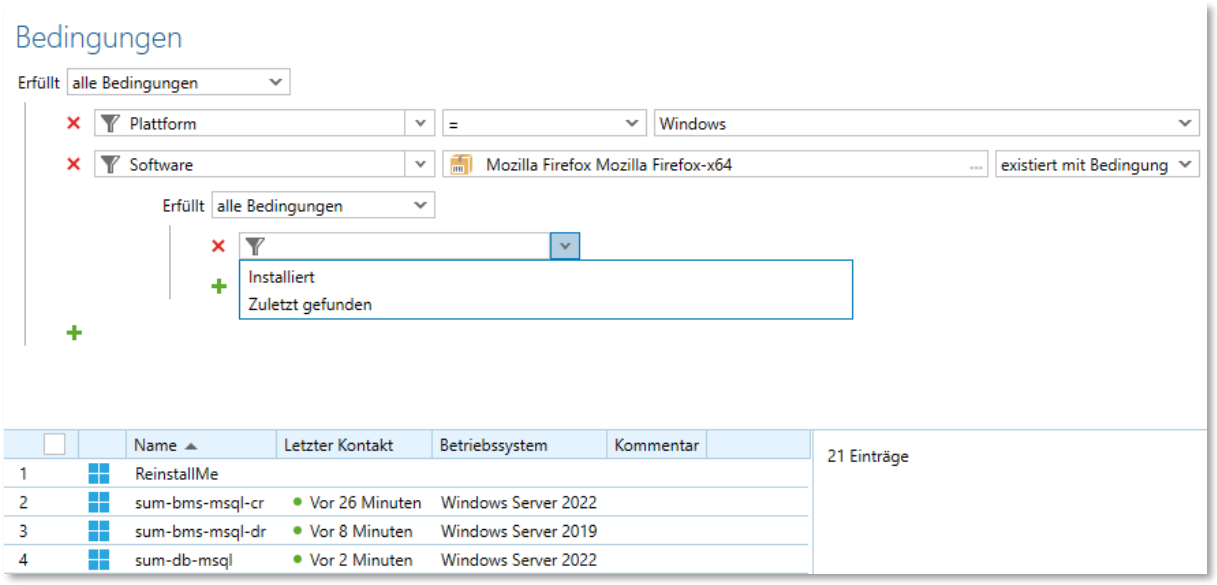


Abbildung 16 – Bedingungen für installierte Software

Mit dieser Bedingung lassen sich nun viele häufig gefragte Szenarien abbilden.
Die Bedingung „Software“ (Windows) ermöglich das Durchsuchen der eigenen Software im Windowsumfeld. Das Dropdown für „existiert/existiert nicht/existiert mit Bedingung" ermöglicht hierbei präzisere Kriterien.

- **existiert**: prüft, ob Endpunkte eine bestimmte Software installiert haben
- **existiert nicht:**
  prüft, ob die gewählte Software auf den Endpunkten fehlt; Dies betrifft eine Installation durch Deploy wie auch die dazu inventarisierte Installation.
- **existiert mit Bedingung**: prüft, ob Endpunkte eine bestimmte Software installiert haben und wenn ja, mit granularen Bedingungen:
  - **wurde installiert vor/nach/am**: nur Installationen mit entsprechendem Installationsdatum; Dies betrifft Installationen durch Deploy, wie auch die „Erst“-Inventarisierung.
  - **wurde zuletzt gefunden vor/nach/am**: prüft, wann die entsprechende Software auf dem Endpunkt zuletzt inventarisiert wurde

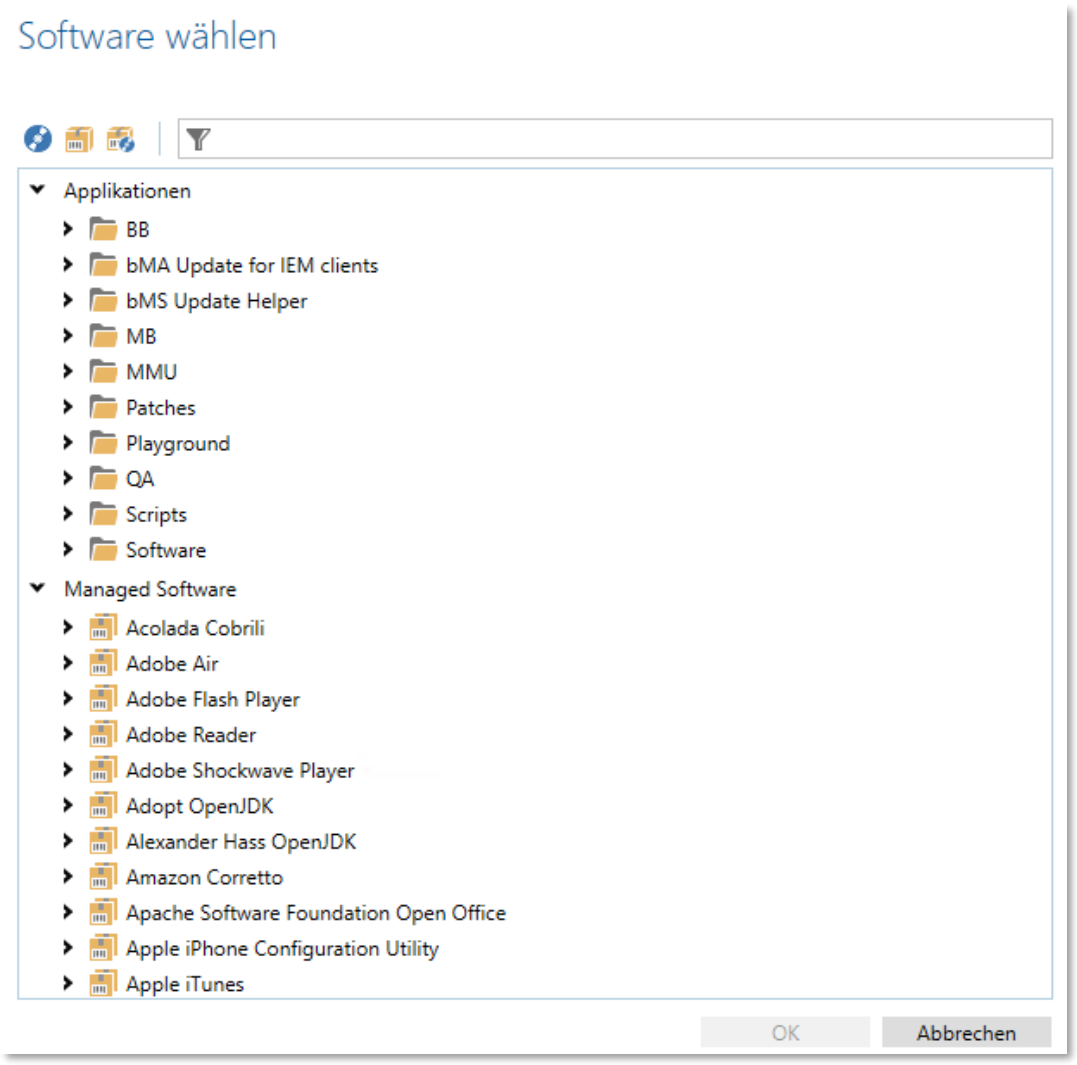


Abbildung 17 – Dialog für die Auswahl der Softwareobjekte in den UDGs

Die Struktur einer baramundi-Umgebung kann sehr spezifisch und auch groß ausfallen. In unseren UDGs gibt es daher einen neuen Dialog zur Auswahl dieser Objekte. Dies ermöglicht die Erstellung dynamischer Gruppen, wie bspw.:

- Liste mir alle Windows Endpunkte auf, auf welchen eine bestimmte Software installiert oder inventarisiert ist.
- Weise automatisch den Job zur „Unternehmensanpassung Chrome“ auf Endpunkten zu, welche Google Chrome-x64 (oder eine beliebige darunter liegende MSW-Version) installiert haben.

1.4.1.2 Jobs

Es ist nun möglich in Universellen Dynamischen Gruppen auch auf die jeweils zugewiesenen Jobs der Endpunkte zu prüfen. Dazu gibt es bei den Eigenschaften einen weiteren Eintrag „Jobzuweisung".

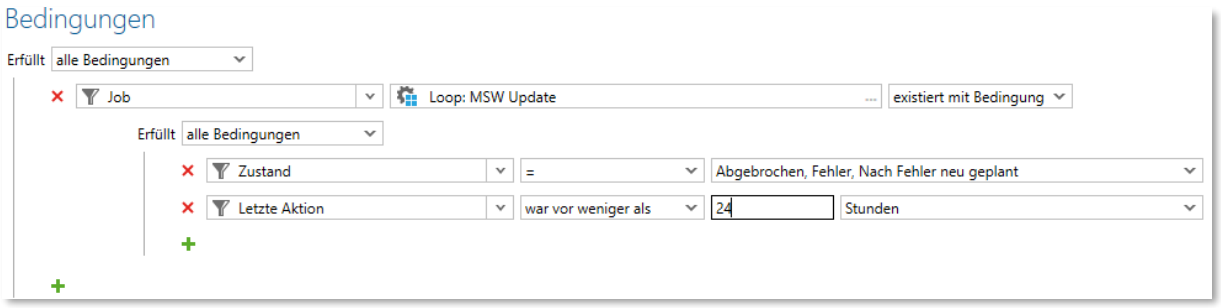


Abbildung 18 – UDG - Neue Bedingung „Jobzuweisung" mit „existiert mit Bedingung"

Nach einem Klick auf das freie Feld öffnet sich anschließend ein Dialog, in dem ein spezifischer Job ausgewählt werden kann. Werden weitere Bedingungen auf der Jobzuweisung konfiguriert, so kann, wie bei UDGs üblich, gewählt werden, ob von diesen Bedingungen alle, mindestens eine oder keine zutreffen sollen.

Es gibt dabei drei Möglichkeiten zum Filtern:

- **existiert**: prüft, ob Endpunkte den gewählten Job zugewiesen haben
- **existiert nicht**: prüft, ob Endpunkte den gewählten Job nicht zugewiesen haben
- **existiert mit Bedingung**: prüft, ob die Zuweisung vorhanden ist, und erlaubt weitere Kriterien auf den Eigenschaften der Jobzuweisung:
    - **Abweisungen durch Benutzer**: Wie häufig hat der Benutzer die Jobausführung abgewiesen?
    - **Ausführungen:** Wie oft wurde der Job ausgeführt?
    - **Erfolgreiche Ausführungen:** Wie oft wurde der Job erfolgreich ausgeführt?
    - **Erstellt**: Wann wurde die Jobzuweisung erstellt?
    - **Fehlerhafte Ausführungen:** Wie häufig war die Ausführung des Jobs nicht erfolgreich?
    - **Letzte Aktion**: Wann gab es die letzte Änderung an der Jobzuweisung?
    - **Nächster Start:** Wann wurde der nächste Start des Jobs eingeplant?
    - **Startzeit:** Wann wurde der Job gestartet?
    - **Wiederholungen nach Fehler:** Wie oft wurde nach einem Fehler versucht, den Job erneut auszuführen?
    - **Zustand**: Welchen Zustand hat die Jobzuweisung? (Dies ist ein Auswahlfeld und erlaubt mehrere gewählte Zustände.)
    - **Zustandsmeldung:** Welcher Text steht in der textuellen Beschreibung des Zustands?

1.4.2 Erweiterung von bConnect

1.4.2.1 Controller-Erweiterungen

1.4.2.1.1 Assets

Auch unsere Schnittstelle bConnect erweitert in diesem Release ihren Funktionsumfang. Bislang waren Assets der baramundi-Umgebung nur über unsere alten (deprecated) Schnittstellen zugänglich. Mit der 2024 R1 können Assets nun über bConnect abgefragt werden. Es gibt den neuen Assets-Controller, der mit dem gewohnten Komfort der Swagger UI zugänglich ist.

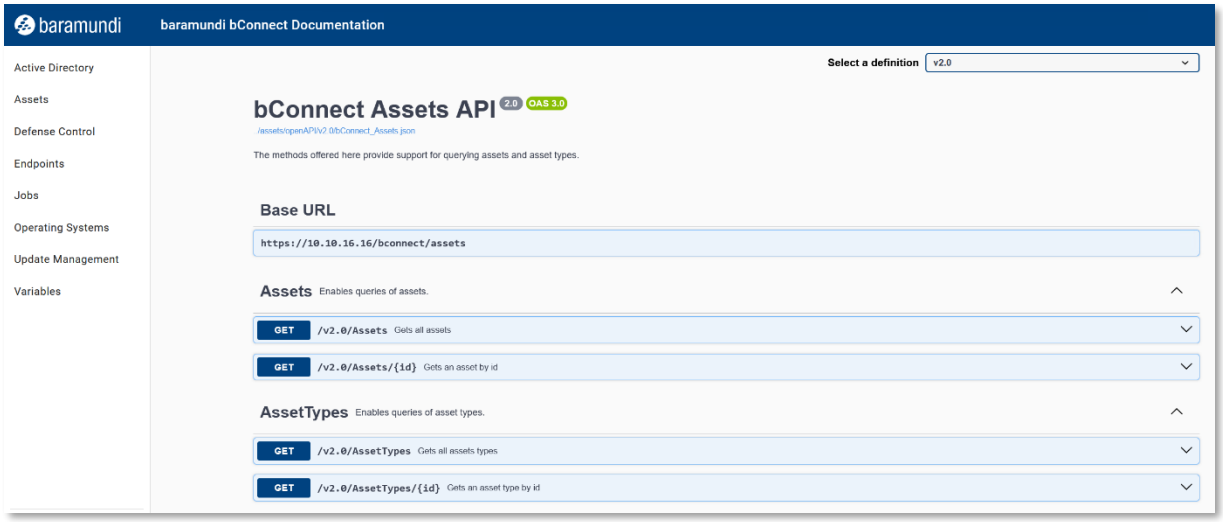


Abbildung 15 – Abfragen der Assets über bConnect

Der Benutzer kann entweder alle Assets oder ein Asset anhand seiner GUID abrufen, erstellen, editieren oder auch löschen. Diese Umstellung ist auch ein weiterer Schritt, die alten Schnittstellen obsolet zu machen.

Die Empfehlung ist daher, weiterhin alle noch aktiven Skripte und Programme, die noch auf httpMOC oder bMOL basieren, zu bConnect zu migrieren.

1.4.2.1.2 Systemsprache

Um dem Vorgang der Aufnahme neuer Endpunkte im internationalen Umfeld noch entgegenzukommen, wurde der bestehende Controller nun um die Systemsprache der Windows-Endpunkte erweitert und kann jetzt über den OperationSystems-Context von bConnect V2 gesetzt werden.

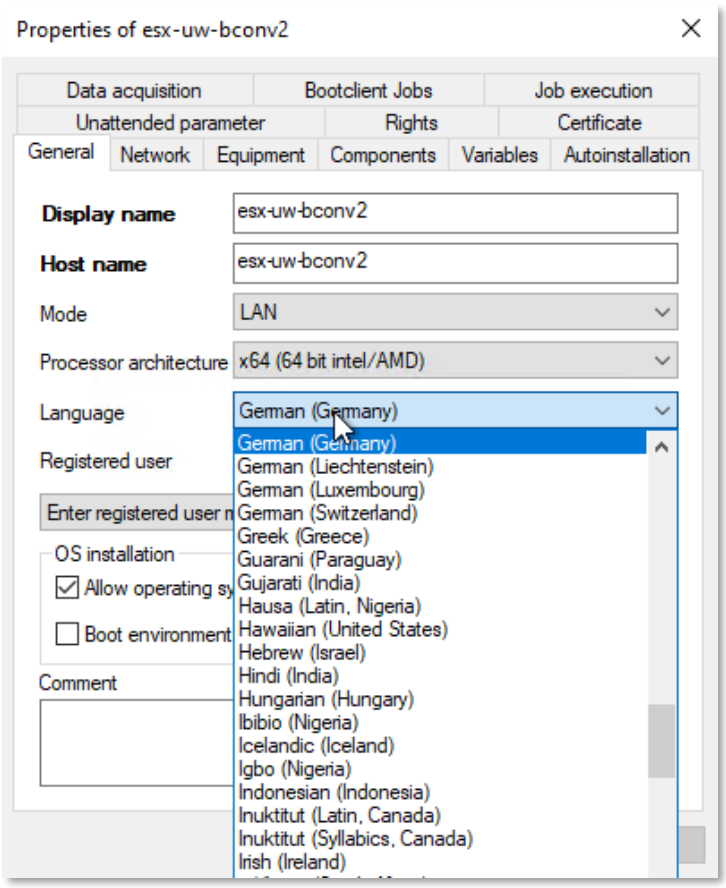


Abbildung 16 – Windows Endpunkt – Sprachauswahl der bMC

1.4.3 Benutzerdefinierte SSH-Inventur

In einem immer größer wachsenden Netzwerk kommt es vermehrt zu Endpunkten, welche entweder wegen ihres Betriebssystems selbst oder aus Sicherheitsgründen rein per SSH erreichbar sind. Auch neue Appliances auf Linuxbasis oder Geräte, auf welchen keine Veränderung (Agent-Installation) stattfinden darf, fallen in diese Kategorie.

Genau für diese Gerätetypen haben wir nun unsere Inventarisierungsmethode erweitert: Es gibt die Möglichkeit, Templates (Vorlagen) zu erstellen und die bis dato von baramundi vorgegebenen Standardbefehle, -parameter und -attribute individuell anzupassen.

Diese neuen Templates für die SSH-Inventur sind nun unter den Inventurtemplates zu finden. So können beispielsweise für ähnliche Geräteklassen eigene, neue SSH-Inventory-Templates erstellt werden.

Im Gegensatz zum Default-Template können in den selbst erstellten Templates vorhandene Kommandos individuell angepasst und benutzerdefinierte Kommandos ganz einfach hinzugefügt werden, um detailliertere Abfragen zu erstellen. Die Nutzung mehrerer Templates kann den Komfort erhöhen, da sie auf die jeweilige Geräteklasse genau angepasst werden können.

Die Templates können dann unterhalb des Jobschritts entsprechend ausgewählt werden.

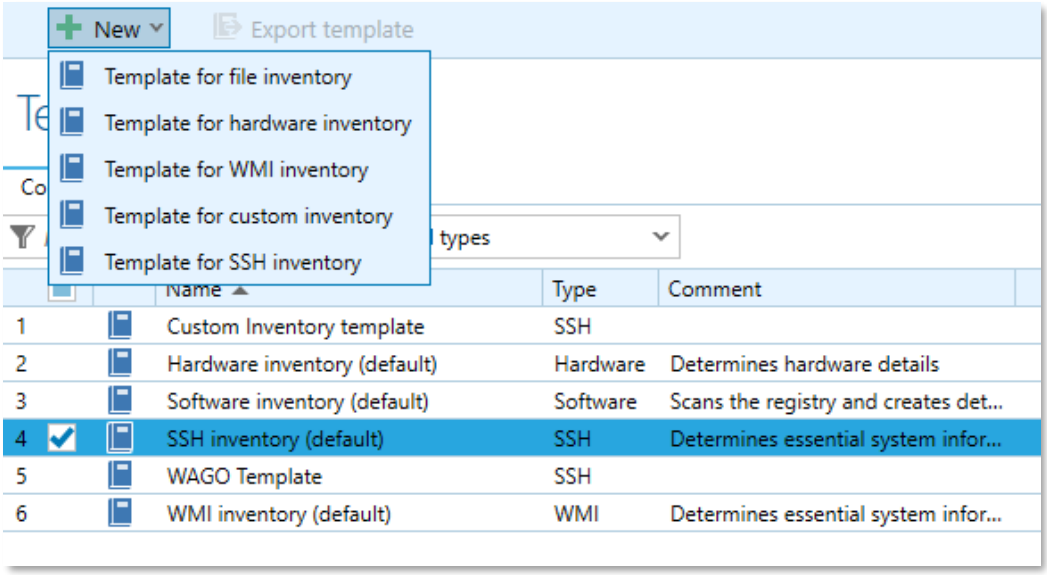
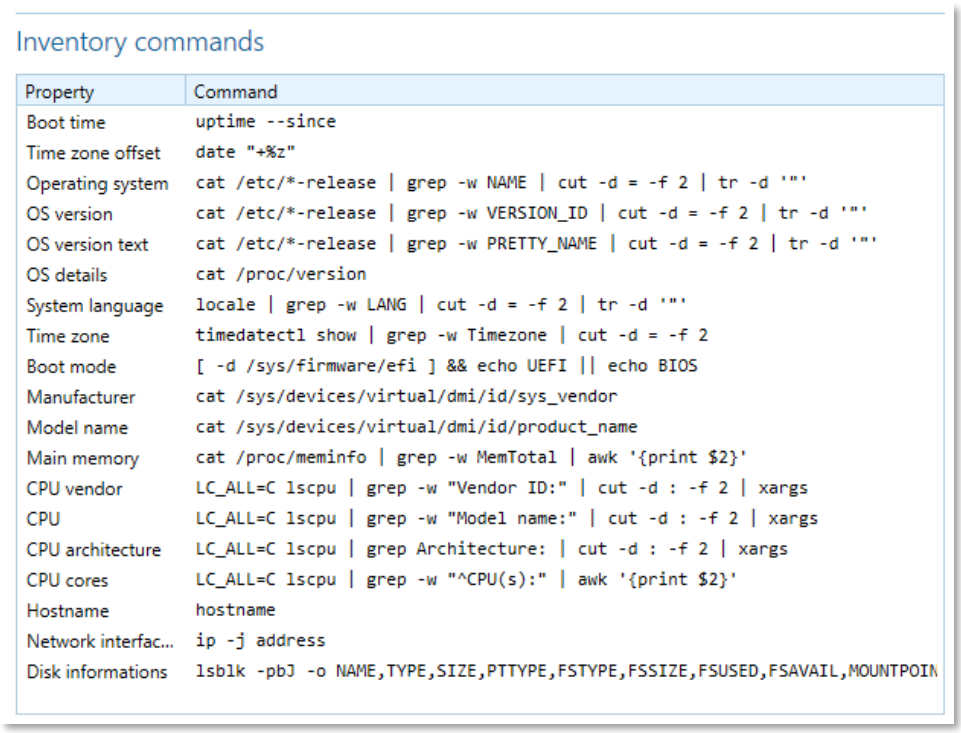


Abbildung 17 – Neue Vorlage – SSH-Inventarisierung

Die einzelnen Kommandos der Inventarisierung entsprechen einer Art benutzerdefinierter Variable. Somit kann pro Wert dies als Eigenschaft mit dem dahinterliegenden Kommando hinterlegt werden. Siehe Screenshot:



Inventory commands

Property	Command
Boot time	`uptime --since`
Time zone offset	`date "+%z"`
Operating system	`cat /etc/*-release | grep -w NAME | cut -d = -f 2 | tr -d '"'`
OS version	`cat /etc/*-release | grep -w VERSION_ID | cut -d = -f 2 | tr -d '"'`
OS version text	`cat /etc/*-release | grep -w PRETTY_NAME | cut -d = -f 2 | tr -d '"'`
OS details	`cat /proc/version`
System language	`locale | grep -w LANG | cut -d = -f 2 | tr -d '"'`
Time zone	`timedatectl show | grep -w Timezone | cut -d = -f 2`
Boot mode	`[ -d /sys/firmware/efi ] && echo UEFI || echo BIOS`
Manufacturer	`cat /sys/devices/virtual/dmi/id/sys_vendor`
Model name	`cat /sys/devices/virtual/dmi/id/product_name`
Main memory	`cat /proc/meminfo | grep -w MemTotal | awk '{print $2}'`
CPU vendor	`LC_ALL=C lscpu | grep -w "Vendor ID:" | cut -d : -f 2 | xargs`
CPU	`LC_ALL=C lscpu | grep -w "Model name:" | cut -d : -f 2 | xargs`
CPU architecture	`LC_ALL=C lscpu | grep Architecture: | cut -d : -f 2 | xargs`
CPU cores	`LC_ALL=C lscpu | grep -w "^CPU(s):" | awk '{print $2}'`
Hostname	`hostname`
Network interfac...	`ip -j address`
Disk informations	`lsblk -pbJ -o NAME,TYPE,SIZE,PTTYPE,FSTYPE,FSSIZE,FSUSED,FSAVAIL,MOUNTPOIN`

Abbildung 18 – SSH-Inventarisierungsvorlage mit Kommandos

Diese Befehle können, wie auch die schon länger vorhandenen, benutzerdefinierten Befehle, einfach mit einem Doppelklick bearbeitet werden.

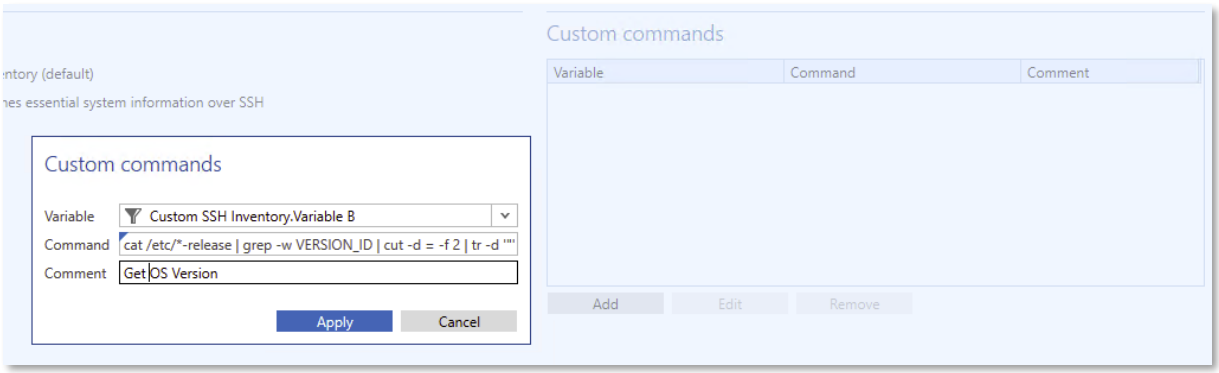


Abbildung 19 – Dialog zum Hinzufügen neuer SSH-Kommandos

1.4.4 Automatische Jobverzögerung bei aktiven Vollbild-/ Präsentationsanwendungen

Der sogenannte „Nicht Stören Modus“ wird in unserer Version 2024 R1 erweitert bzw. wird ermöglicht den Tray Notifier dynamischer auf die Benutzeraktivitäten zu reagieren. Wenn Windows uns mitteilt, dass keine Störung erwünscht ist, dann legen wir den Tray Notifier somit „schlafen“. Dies wird bspw. im Vollbildmodus gesendet, was hilfreich ist bei aktuell stattfindenden, geteilten Präsentationen. Der baramundi Tray Notifier macht sich dann erst anschließend bemerkbar.

Hierbei wird auf eine Windows Funktion zurückgegriffen, welche nicht nur die Präsentationen erkennt, sondern ebenso Szenarien wie Bildschirmschoner, andere Vollbildanwendungen oder Direct3D-Anwendungen.

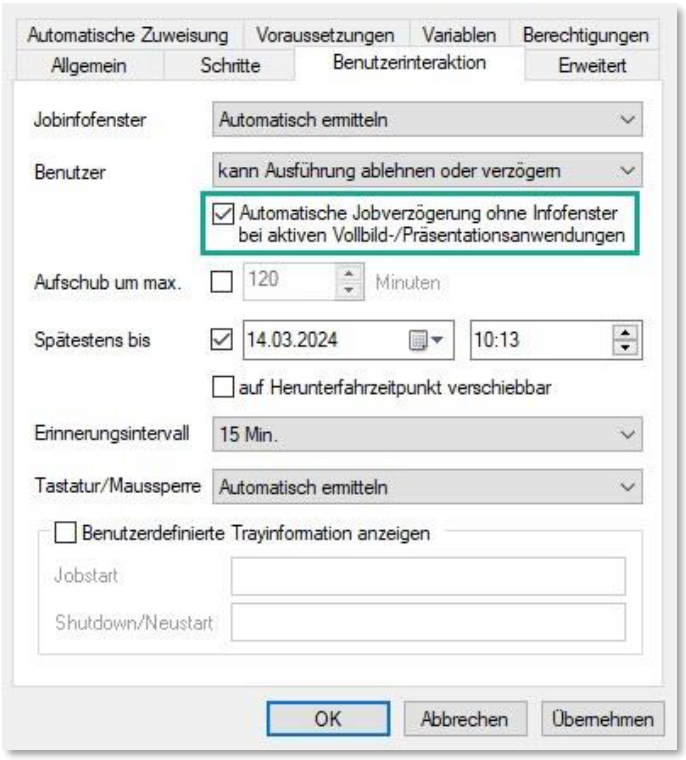


Abbildung 20 – Konfigurationsmöglichkeiten im Job

Die neue Option ist standardmäßig bei einem neuen Job aktiviert, sofern der Benutzer Einfluss auf die Jobausführung hat.

Eine Ausnahme gibt es: Wenn die maximale Aufschubzeit erreicht wurde, dann wird das Job-Infofenster dennoch über dem Vollbild angezeigt.

1.4.5 Identifizierung von Endpoints anhand UUID

Der Universal Unique Identifier – kurz UUID – wird bei modernen Computern in der Firmware (UEFI) hinterlegt und ermöglicht die eindeutige Identifizierung des Systems. Im Kontext des Endpoint Managements ist es unerlässlich, die Ziele für die durchzuführenden Managementaktionen zweifelsfrei zu identifizieren, um nicht, zum Beispiel, versehentlich den falschen Endpoint zurückzusetzen.

Ist ein baramundi Management Agent installiert, verwendet die bMS ein clientseitiges Zertifikat, um die Identität zu bestätigen – was aber, wenn ein System neu installiert werden soll und noch kein Agent installiert ist? In diesem Fall wird bisher beim Netzwerkboot die MAC-Adresse der Netzwerkkarte verwendet. Mit zunehmend schlankerer Hardware sind häufig keine Netzwerkanschlüsse mehr an den Geräten zu finden. So müssen externe Netzwerkadapter in Form von Dongles oder Docking Stations verwendet werden, welche eine eindeutige Identifizierung anhand der MAC-Adresse erschweren.

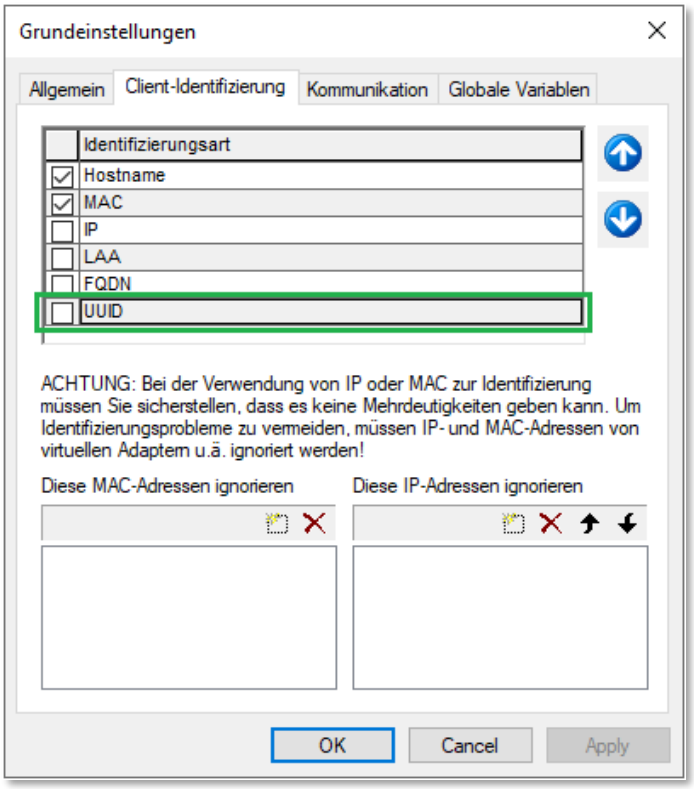


Abbildung 21 – Client-Identifizierung mit neuem Feld für UUID

Die bMS unterstützt nun die UUID als primäres Identifikationsmerkmal. Bei neu angelegten Datenbanken wird die UUID automatisch als Identifikationsmerkmal gesetzt. Bei bestehenden Datenbanken wird die UUID im Rahmen des Updates als Merkmal verfügbar gemacht, aber nicht aktiviert.

Hinweis: *In Umgebungen, welche mit der bMS 2023 R2 UUID als Technical Preview aktiviert hatten, muss die UUID erneut als primäres Identifikationsmerkmal konfiguriert werden – die Einstellungen aus dem Technical Preview werden nicht migriert.*

1.5 Systemanforderungen und Kompatibilität

1.5.1 baramundi Management Server und baramundi PXE Relay

- unterstützte Plattformen: siehe 1.5.17 (Spalte bMS)
- .NET Core 6.x, Asp.Net Core Framework 6.x und .NET Core Desktop 6.x in gleichen Versionen wird vorausgesetzt.
- unterstützte Sprachen: Deutsch und Englisch
- Es wird empfohlen, einen dedizierten Server für den Betrieb des baramundi Management Servers zu verwenden.
- Für den baramundi Management Server müssen bestimmte Ports verfügbar sein[3].
- Eine Einbindung in eine Windowsdomäne - Windows Active Directory - wird empfohlen.
- Hardwareanforderungen Server/Netzwerk:
    - verfügbarer Arbeitsspeicher: mindestens 8 GB; empfohlen 16 GB
    - Prozessor: mindestens 4 Kerne
    - Speicherplatz zur Installation der bMS: mindestens 5 GB
    - Netzwerkkarte: Mindestens 1 Gigabit

1.5.2 Datenbankanbindung

- Unterstützte Plattformen:
    - SQL-Server 2022
    - SQL-Server 2019
    - SQL-Server 2017
    - SQL-Server 2016 SP3 (deprecated)
    - Oracle 19c (deprecated)
      Hinweis: bMS-Versionen ab 2025 R2 sind mit Oracle Datenbanken nicht mehr kompatibel. Ein Umstieg auf MS-SQL oder unsere künftige Cloud Lösung (bMSaaS) wird empfohlen.
- mindestens 10 GB Festplattenplatz für die baramundi Datenbank
- Der baramundi Management Server ist ein datenbankorientiertes System. Daher ist auf ausreichend Performance der Datenbank und eine performante Anbindung zu achten.

[3] Eine Liste der am Server genutzten Ports steht in unserer Onlinehilfe https://docs.baramundi.com zur Verfügung.

- Bei Umgebungen bis zu 250 Clients kann die SQL Express Edition verwendet werden.
- Ein Betrieb des Datenbankservers und des baramundi Management Servers auf einem System ist zulässig. Bei höheren Anforderungen und größeren Umgebungen wird ein eigenständiger Datenbankserver empfohlen.

1.5.3 baramundi Management Center

- unterstützte Plattformen für das baramundi Management Center, sowie die Add-Ons Automation Studio, License Management, Remote Control und ImageMount: siehe 1.5.17 (Spalte bMC)
- Microsoft Edge WebView2 Runtime ist erforderlich.
- Bildschirmauflösung:
  - Mindestbildschirmauflösung 1024 x 768 Pixel
  - Empfohlen wird eine Auflösung von 1280 x 800 Pixel oder höher.
  - Alle Auflösungen beziehen sich auf eine Schriftgrößendarstellung von 100%.

1.5.4 baramundi OS Customization Tool

- Dieses per Managed Software bereitgestellte baramundi Management Center Add-On zur Anpassung von Windows 10 oder Windows 11 Images wird auf den in MSW ersichtlichen Plattformen unterstützt.
- Zur Anpassung der Windows Images ist das Microsoft ADK für Windows 11 erforderlich.

1.5.5 baramundi DIP

- unterstützte Plattformen: siehe 1.5.17 (Spalte bDIP)
- .NET Core 6.x, Asp.Net Core Framework 6.x und .NET Core Desktop 6.x in gleichen Versionen wird vorausgesetzt.
- Empfohlen wird zusätzlicher Festplattenspeicherplatz:
  - 10 GB für Applikationen
  - 90 GB für Managed Software (MSW)
  - 6 GB für jedes Betriebssystem, das mit dem Modul baramundi OS-Install verteilt werden soll.

1.5.6 baramundi Gateway

- unterstützte Plattformen: siehe 1.5.17 (Spalte bGW)

- Es wird empfohlen das baramundi Gateway nicht zusammen mit anderen Diensten auf dem gleichen System zu betreiben.
- Eine Einbindung in ein Active Directory ist nicht notwendig.
- Das baramundi Gateway sollte in einer DMZ-Umgebung betrieben werden, um eine strikte Trennung zum bMS Server zu gewährleisten. Ein Betrieb von baramundi Gateway und bMS auf einem System wird nicht unterstützt.
- Hardwareanforderungen Server/Netzwerk:
    - verfügbarer Arbeitsspeicher: mindestens 4 GB; empfohlen 8 GB
    - Speicherplatz zur Installation des baramundi Gateway: mindestens 1 GB
    - Netzwerkkarte: mindestens 1 Gigabit

1.5.7 baramundi OS Install

- Zur Anpassung der Windows Images ist das Microsoft ADK für Windows 11 erforderlich.
- Das ADK steht in Managed Software als ADK10, Version 2209 zur Verfügung.

1.5.8 baramundi License Management

- Die Ablage von Lizenzdokumenten in der Datenbank kann großen Speicherbedarf auf dem Datenbankserver verursachen.
- Der MS-SQL Express Datenbankserver ist von Microsoft auf 10 GB Datenbankgröße begrenzt. Daher wird die Verwendung für baramundi License Management nicht empfohlen.
- baramundi License Management unterstützt die folgenden Browser, jeweils in der aktuellen Version:
    - Microsoft Edge
    - Google Chrome
    - Mozilla Firefox

1.5.9 baramundi Schnittstellen

- bConnect steht in der Version 1.1 sowie 2.0 zur Verfügung.
- Deprecated - Die Schnittstelle bMOL (baramundi Management Object Language) wird nicht mehr weiterentwickelt. Wir empfehlen die Umstellung und Verwendung unserer Schnittstelle bConnect.
  Hinweis: Die Schnittstelle bMOL wird ab bMS Version 2025 R1 nicht mehr verfügbar sein.
- Deprecated – Die Schnittstelle httpMOC wird nicht mehr weiterentwickelt. Wir empfehlen die Umstellung und Verwendung unserer Schnittstelle bConnect.
  Hinweis: Die Schnittstelle httpMOC wird ab bMS Version 2025 R1 nicht mehr verfügbar sein.
- Deprecated – Der direkte Zugriff auf die Datenbank (SQL/Oracle) wird nicht unterstützt. Wir empfehlen die Umstellung und Verwendung unserer Schnittstelle bConnect.
  Hinweis: Die DB-Doku wird ab 2023 R2 nicht mehr mit ausgeliefert.

*) Deprecated: Es erfolgen keine Featureupdates und Bugfixes mehr. Kritische Sicherheitsupdates werden für die aktuelle Version zur Verfügung gestellt.

1.5.10 baramundi Network Devices

- unterstützte Plattformen: siehe 1.5.17 (Spalte bND)
- Der Networkscanner ist ein Add-On zum Windows bMA. Er steht allen Kunden über Managed Software zur Verfügung.
- .NET 4.7.2 wird vorausgesetzt.

1.5.11 baramundi OT Devices

- Datenerfassung erfolgt per SNMP Version1, Version2c, Version3
- Unterstütze Plattformen: Siemens SIMATIC S7 1200 und 1500

1.5.12 baramundi Kiosk

- Unterstützte Plattformen: siehe 1.5.17 (Spalte bMA)
- Zur Benutzeranmeldung und Jobzuordnung auf Benutzerbasis ist ein Windows Active Directory inklusive eingerichtetem baramundi AD-Sync notwendig.
- baramundi Kiosk unterstützt die folgenden Browser, jeweils in der aktuellen Version:
  - Microsoft Edge
  - Google Chrome
  - Mozilla Firefox

1.5.13 Unterstützung von Android

- Unterstützte Versionen:
  - Android Enterprise 14
  - Android Enterprise 13
  - Android Enterprise 12
  - Android Enterprise 11
  - Android Enterprise 10
  - Android Enterprise 9
  - Android Enterprise 8 *)
  - Android Enterprise 7 *)

*) Dieses Betriebssystem wird nur eingeschränkt unterstützt. Das kann bedeuten, dass neue Funktionen auf diesem Betriebssystem nicht nutzbar sind oder Funktionen nicht mehr wie bisher verwendet werden können. Kein Support für Zero-Touch.

1.5.14 Unterstützung von iOS

- Unterstützte Versionen:
  - iOS Version 17
  - iOS Version 16
  - iOS Version 15
  - iOS Version 14
  - iOS Version 13
  - iOS Version 12

1.5.15 Unterstützung von Linux

- Die SSH-Inventur auf Linux-Geräten wurde auf folgenden Betriebssystemen mit dem default Template getestet:
    - Debian: Version 11 und 12
    - OpenSuse: ab Version 15
    - Ubuntu Server: Version 21 und 22
- Durch die individuelle Anpassung von Templates können die Befehle entsprechend vom Benutzer angepasst werden, um individuelle Kompatibilität mit weiteren Betriebssystemen zu erreichen.

1.5.16 Unterstützung von macOS

- Unterstützte Versionen:
    - macOS 14.x (Sonoma)
    - macOS 13.x (Ventura)
    - macOS 12.x (Monterey)
    - macOS 11.x (Big Sur)
    - macOS 10.15 (Catalina)

1.5.17 Unterstützung von Windows

- bMS/R: baramundi Management Server, baramundi PXE Relay
- bMC: baramundi Management Console,
  inclusive bRemote, ImageMount und License Management AddOn
- bAS baramundi Automation Studio
- bGW: baramundi Gateway
- bDIP: baramundi DIP, bBT und DipSync Dienst
- bMA: baramundi Agent für Windows
- bND: baramundi Networkscanner als Add-On zum Windows bMA
- X: Vollständig unterstützt.

Plattformbezeichner	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2022 Standard/Datacenter (Desktopdarstellung)	X	X	X	X	X	X	X
Windows Server 2022 Standard/Datacenter (Core)						X	
Windows Server 2019 Standard/Datacenter (Desktopdarstellung)	X	X	X	X	X	X	X
Windows Server 2019 Standard/Datacenter (Core)						X	
Windows Server 2016 Standard/Datacenter (Desktopdarstellung)	X	X	X	X	X	X	X
Windows 11 Pro / Enterprise (N)		X	X		X	X	X
Windows 10 Pro / Enterprise 22H2 (N) (32 Bit und 64 Bit)		X	X		x64	X	X
Windows 10 Pro / Enterprise 21H2 (N) (32 Bit und 64 Bit)		X	X		x64	X	X
Windows 10 Enterprise 2021 LTSC (32 Bit und 64 Bit)		X	X		x64	X	X
Windows 10 Enterprise 2019 LTSC (32 Bit und 64 Bit)		X	X		x64	X	X
Windows 10 Enterprise 2016 LTSB (32 Bit und 64 Bit)		X	X		x64	X	X
Windows 10 Enterprise 2015 LTSB (32 Bit und 64 Bit)		X	X		x64	X	X

1.5.18 Unterstützung von Windows mit Einschränkungen

Die folgenden Betriebssysteme werden von den baramundi-Komponenten nur eingeschränkt unterstützt. Das kann bedeuten, dass neue Funktionen auf diesem Betriebssystem nicht nutzbar sind oder Funktionen nicht mehr wie bisher verwendet werden können. Aufgrund der Komplexität und Vielzahl der Altsysteme kann baramundi die Funktionalität auf diesen Systemen nicht gewährleisten. Aufgrund der Einschränkungen empfehlen wir den Einsatz modernerer Betriebssysteme. Auf Betriebssystemen, welche außerhalb des Mainstreamsupports von Microsoft sind, können wir keine Unterstützung der baramundi Serverkomponenten mehr leisten (bMS/R, bMC, bAS, bGW, bDIP).

- (1): Wird nur noch eingeschränkt unterstützt, da Microsoft den (grundlegenden) Produktsupport beendet hat.
- (2): Ein aktueller bMA kann auf Windows XP nicht ausgeführt werden. Beim Einsatz von sind diese Hinweise zwingend zu beachten: 1.7.15 Windows Agent (bMA) Hinweis für Windows XP
- (3) Kein Support mehr ab bMS 2024 R2.

	bMS/R	bMC	bAS	bGW	bDIP	bMA	bND
Windows Server 2012 R2 Standard/Datacenter (Server mit grafischer Benutzeroberfläche)						1	1
Windows Server 2012 Standard/Datacenter (Server mit grafischer Benutzeroberfläche)						1	1
Windows Server 2008 R2 SP1 Standard /Enterprise / Datacenter						3	3
Windows 10 Pro / Enterprise 1703 bis 21H1 (N) (32 Bit und 64 Bit)						1	1
Windows 8.1 Pro / Enterprise (32 Bit / 64 Bit)						1	1
Windows 7 SP1 Professional/Enterprise/Ultimate (N) (32 Bit und 64 Bit)						1	1
Windows XP SP3 (32 Bit)						2	

1.5.19 Sprachen

Das baramundi Management Center, baramundi License Management sowie das Automation Studio sind in folgenden Sprachen verfügbar:

Deutsch, Englisch

Der bMA für Windows-Clients unterstützt Benutzernachrichten in folgenden Sprachen:

Deutsch, Englisch, Bulgarisch, Chinesisch, Dänisch, Finnisch, Französisch, Griechisch, Italienisch, Niederländisch, Norwegisch, Polnisch, Portugiesisch, Rumänisch, Russisch, Schwedisch, Slowakisch, Spanisch, Türkisch, Tschechisch, Ungarisch

Der baramundi Kiosk unterstützt die folgenden Sprachen:

Deutsch, Englisch, Polnisch

Weitere Sprachen können durch die Administration hinzugefügt werden.

Für alle serverseitigen Dienste (d.h. baramundi Management Server, baramundi Gateway, DIP) werden folgende Sprachen unterstützt:

Deutsch, Englisch

1.6 Produktverbesserungen im Detail

1.6.1 Umgesetzte Abkündigungen / Entfernte Eigenschaften

- Patchupdates über den Jobschritt `Microsoft Patches verteilen (Classic)` sind abgekündigt. Die Bereitstellung der Patchdaten `bpmdata3_reduced_signed.zip/bpmdata3_ signed.zip` wurde im April 2024 eingestellt.
- Windows Vista und Windows Server 2008 SP2 werden nicht mehr unterstützt.
- MS-SQL Server 2014 wird nicht mehr unterstützt.
- Android Version 4.0.4. bis Version 9 wird nicht mehr unterstützt.
- Samsung KNOX auf Android Version 4.0.4 bis Version 9 wird nicht mehr unterstützt.

1.6.2 Allgemein, beim Anlegen einer neuen baramundi Datenbank

- Die Server-Grundeinstellung sind bei neuen Datenbanken jetzt:

```
Client-Identifizierung      Hostname, UUID, MAC
IP-Gültigkeitsdauer         192
Verbindungsmodus            IP-Adresse wenn vorhanden
ICMP                        ja
```

- Unter Einstellungen-Jobausführung ist die `Anzahl max. gleichzeitig aktiver Clients` jetzt `250`.
- Beim Anlegen neuer baramundi Datenbanken ist es jetzt möglich die für Energymanagement verwendete Währung zu setzen.
- Bei der `logischen Gruppierung` ist jetzt kein `DIP` hinterlegt.

1.6.3 Windows Agent (bMA)

- Die Passwortlänge für das automatisch generierte Passwort für den lokalen Installationsbenutzer (baraInstLocal) wurde von 14 auf 64 Zeichen erhöht.
- Bugfix: In seltenen Fällen bleibt nach dem Aufheben der Tastatur und Maussperre das Infofenster des baramundi Traynotifier dauerhaft sichtbar und blockiert u.U. eine Abmeldung.

1.6.4 Management Center (bMC)

- Unter `Konfiguration – Variablen` zeigt das neue Feld `Verwendung` an, wie diese Variable referenziert werden kann. Kopieren ist hier ebenfalls möglich.
- Das Menü für die PXE-Konfiguration wurde umgestellt und ist jetzt unter `bMC – Konfiguration - Server – PXE-Unterstützung` zu finden. Dort kann die `Client-Identifizierung` jetzt von `MAC` auf `UUID` umgestellt werden. Siehe dazu Anmerkung 1.7.13.
- Unter `bMC – Konfiguration - Server – Einstellungen – Grundeinstellungen` ist für die `Client-Identifizierung` jetzt auch UUID möglich.
- Unter `bMC – Job – Eigenschaften – Benutzerinteraktion` ist jetzt die Option `Automatische Jobverzögerung ohne Infofenster bei aktiven Vollbild-/Präsentationsanwendungen` verfügbar. Damit erscheint auf dem Client kein Jobinfo-Fenster, wenn z.B. eine PowerPoint-Präsentation erkannt wurde. Wird die Präsentation beendet, so erscheint das Infofenster nach einigen Minuten.
- Unter `bMC – Konfiguration - Server – Einstellungen – Jobausführung` wurde die Option `Jobtargets mit ungültigen Status beim Modulstart aufräumen` entfernt.
- In einer `Dynamische Gruppe (Universell)` steht jetzt die Bedingung `Software` zur Verfügung und ermöglicht damit detaillierte Abfragen auf installierte (`existiert`) oder fehlende (`existiert nicht`) Applikationen.
- In einer `Dynamische Gruppe (Universell)` steht jetzt die Bedingung `Job` zur Verfügung und ermöglicht damit Abfragen auf erfolgreiche/nicht erfolgreiche Jobausführungen inklusive der Angabe von Zeitpunkten.
- Wird eine Applikation neu angelegt, so sind als `Unterstützte Betriebssysteme` nur noch die Client Betriebssysteme Windows 10/11 und die Server Betriebssysteme ab 2016 per Default angewählt.
- Wird eine Applikation neu angelegt, so ist jetzt per Default die Option `bBT unterstützten` aktiv.
- Die Unterknoten unter `bMC – Konfiguration` sind jetzt zugeklappt.

- Bugfix: Eine `Dynamische Gruppe (Universell)` kann nicht gespeichert werden, wenn Variablen vom Typ Datum in einer Bedingung verwendet werden. Es erscheint eine Exception „Could not cast..“
- Bugfix: unter `Client – Inventur – Inventarisierungen` arbeitet die Aktion `Zurück zur Übersicht` nicht. Sie wurde entfernt.
- Bugfix: Die Aktion `Client – Management Agent – Aktiviere Modus Dynamisch` schlägt fehl, wenn der bMC-User keine Rechte für `Konfiguration – Server – Einstellungen` hat.
- Bugfix: Wird der unter `Persönliche Einstellungen – Standard Job-Ordner` angegebene Ordner gelöscht, so kommt es bei Verwendung z.B. der Aktion Installationsjob anlegen zu einer Fehlermeldung „Der Knoten mit der ID wurde nicht gefunden“.

1.6.5 bRemote

- Um bRemote für eine Aufschaltung auf Windows-PE zu verwenden, ist jetzt am `Client – Benutzermenü` der Befehl `Connect to PE` dazu vorhanden.
- Hinweis: Die Unterstützung für Windows XP wurde entfernt.

1.6.6 Remote Desk (AnyDesk)

- Das bMA Setup beinhaltet die AnyDesk*.exe Dateien, diese werden jetzt nachträglich schnell und ohne den Benutzer zu stören im bMA Ordner abgelegt, wenn die erste Aufschaltung mit Remote Desk erfolgt.
- Das bMC Setup beinhaltet die AnyDesk*.exe Dateien, diese werden jetzt nachträglich bei der ersten Verwendung von `Client – Fernwartung` installiert. Um diese Aktion durchzuführen, benötigt der bMC Anwender Administrative Rechte. Über den Setupparameter `ManagementCenter_setup.exe /qn ADDLOCAL=ALL` kann AnyDesk*.exe automatisch mitinstalliert werden.
- Bugfix: Werden unter `bMC-Persönliche Einstellungen – Anzeigenamen` Sonderzeichen (z.B. aus der Extended ASCII Tabelle) verwendet, so kann dieser Benutzer keine Fernwartung durchführen. Wird eine Aufschaltung ausgelöst, so wird beim Benutzer des Endgeräts auch keine Nachricht angezeigt. Die Verbindung bricht nach einiger Zeit bMC-Seitig mit dem Fehler „Verbindungsfehler“ ab.

- Bugfix: Beim Verwenden von `Client – Fernwartung` erscheint eine Fehlermeldung „*Value can not be null*“, wenn der bMC-Benutzer kein Profilbild hinterlegt hat. Tritt nur bei Verwendung einer Oracle Datenbanken auf.

1.6.7 Defense Control

- Der Feature „Lokale administrative Benutzerkonten“ kann unter `bmc – Defense Control – Lokale administrative Benutzerkonten` konfiguriert werden.
- In der bMC kann am Client unter `Endpunktsicherheit – Lokales administratives Benutzerkonto` das automatisch generierte Passwort verwaltet werden. Vorausgesetzt der bMC-Benutzer hat für diesen Client das neue Recht `Special – Lokales administratives Konto` und das Feature ist global angeschaltet.
- Bugfix: In seltenen Fällen zeigt die Ansicht `Client – Microsoft Defender Antivirus – Bedrohungen` eine Fehlermeldung „Es werden nicht alle benötigten Servermodule ausgeführt“ an, obwohl alle Servermodule korrekt laufen.

1.6.8 Update Management

- Bugfix: In manchen Fällen wird eine am Job hinterlegte `Persönliche Benachrichtigung` im Fehlerfall bei einem Job mit `Microsoft Update verwalten` Schritten nicht verschickt.
- Bugfix: Das konfigurierte `Standart-Updateprofil für neue Geräte` wird einem neuem Client nicht zugewiesen, wenn dieser über die Client-Erfassung unter PE erfasst wird.

1.6.9 OS-Install

- Im `Boot Media Wizard` ist jetzt der baramundi Server als FQDN automatisch hinterlegt.
- Beim Anlegen eines neuen Betriebssystems ist jetzt bei `Computerkonto vor Installation neu erstellen` voreingestellt.
- Ein über die bMC-Aktion `Client – Extra – Neu installieren` erzeugter Job enthält jetzt am OS-Schritt die Aktion `Abschließend Client` neu starten.
- Die Größe der WindowsRecovery (WinRE)-Partition ist jetzt 1024 MB.

- Bugfix: Wird ein Client über die Automatische MAC Erfassung beim PXE-Boot über ein PXE-Relay erfasst, so ist dieser Client u.U. erst nach Neustart des QueryService in der bMC sichtbar.

1.6.10 baraDIP

- Um bei bBT eine Multidomänenauthentifizierung komfortabler zu unterstützen können jetzt unter `bMC – Konfiguration – DIP – DIP-Verwaltung` am einzelnen DIP-Server zusätzliche `Client-Domänen für bBT-Download` angegeben werden.
- baraDIP verwendet keinen Apache-Webserver mehr.
- Hinweis: baraDIP sperrt jetzt Dateien, während diese vom DipSync übertragen, oder von Client per bBT heruntergeladen werden.
- Bugfix: Ist unter `bMC – Konfiguration – Server – Einstellungen – Downloader` unter `Proxy verwenden` ein Proxy eingetragen, so ist u.U. die TLS Konfiguration für DIP-Server nicht möglich.
- Bugfix: Treten bei der Netzwerkkommunikation auf DIP-Servern Störungen auf, so wurde beobachtet dass der baraDIP-Dienst u.U. in einen Zustand übergeht, wo der Dienst zwar noch laufend ist, jedoch keine Synchronisation mehr durchführt.

1.6.11 Mobile Devices

- Die von Apple Ende 2023 eingeführten „Schnellen Sicherheitsmaßnahmen“ sind als `Patch Level` verfügbar und können auch unter `Compliance – Mobile und macOS-Geräte – Regeln` verwendet werden.
- WPA3 Personal/Enterprise wird jetzt für iOS/iPadOS ab Version 16 unterstützt.
- WPA3 Personal wird jetzt für Android Enterprise ab Version 11 unterstützt.
- WPA3 Enterprise wird jetzt für Android Enterprise ab Version 12 unterstützt.
- Die EAP-Methode `TTLS mit PAP` wird in WiFi-Profilen für iOS/iPadOS und Android Enterprise unterstützt.

- Bei MDM-Profilen ist unter `Einschränkungen - iOS/iPadOS - Spezifische Einstellungen für Geräteregistrierung verwenden` die Option `Installation alternativer Marktplatz-Apps verbieten` verfügbar. Nutzbar ab iOS 17.4.

- Unter `Job - Befehl ausführen` ist für iOS eine Vorlage zum Setzen der Zeitzone vorhanden.

- Neue Profil-Einschränkung `Aktivierung oder Zugriff auf Debugging-Funktionen verbieten` für Android-Enterprise Geräte verfügbar.

- Der Push zu Android-Geräten arbeitet jetzt über den baramundi Cloud-Dienst. Daher ist die Konfiguration der `Google Sender-ID` und `Serverschlüssel` unter `Konfiguration – Mobile Devices – Allgemein – Google Android` nicht mehr notwendig und wurde entfernt.

- Bugfix: Wird die Anzahl an lizenzierten Geräte beim Enrollment eines iOS Geräts erreicht, so schlägt das Enrollment bei der Anmeldung am baramundi bMD Agent fehl und das Gerät wird aus der Verwaltung entfernt.

- Bugfix: Ein bMC Nutzer ohne Leserechte auf `Konfiguration – Mobile Devices – Allgemein` kann an mobilen Endgeräten unter `Inventur – Installierte Apps` und unter `Software – Apps` keine Apps sehen.

- Bugfix: Jobs mit der Option `Neuen Geräten Zuweisen` werden neu enrollten Geräten nicht zugewiesen, wenn diese über Android Zero-Touch enrollt wurden.

- Bugfix: Beim Hinzufügen einer Android-App über den google-Store erschien in seltenen Fällen eine Meldung „Mindestens ein Fehler ist aufgetreten“ oder die Meldung „Der Wert darf nicht NULL sein“.

1.6.12 Netzwerkgeräte

- Unter `Inventur – Vorlagen` ist eine neue Vorlage zur Erkennung von Netzwerkgeräten `SSH-Inventarisierung (Standard)` vorhanden.

- Über `Inventur – Vorlagen – Neu - Vorlage für SSH-Inventarisierung` kann eine eigene Inventurvorlage erzeugt werden. Damit ist es möglich die vorgegebenen `Inventurbefehle` anzupassen oder eigene zu ergänzen.

- Bugfix: Der JobSchritt Inventur über SSH steht nicht zur Verfügung, wenn eine Network Device Lizenz, jedoch keine OT-Inventory Lizenz vorhanden ist.

1.6.13 macOS

- WPA3 wird jetzt für macOS ab Version 13 unterstützt.
- Die EAP-Methode `TTLS mit PAP` wird in WiFi-Profilen auf macOS unterstützt.
- Bugfix: Bei macOS 14.0 wird das baramundi Agent Symbol in der Menüleiste nicht angezeigt. Hinweis: Ein erneutes Zuweisen eines Jobs mit Schritt `SSH-Schnitt-stelle aufnehmen` behebt das fehlende Icon in der Menüleiste.

1.6.14 bConnect

- Das Anlegen und Löschen von Asset-Typen ist jetzt möglich.
  Hinweis: Bei `additionalProperties` eines AssetTypes wird aktuell nur der Typ `String` unterstütz.
- Anlegen, Verändern und Löschen von Assets ist jetzt möglich.
- Der Wert `Client – Eigenschaften – Allgemein – Sprache` kann jetzt auch über bConnect verändert werden.

1.7 Hinweise und bekannte Einschränkungen

1.7.1 Abkündigungen

- Windows Vista und Windows Server 2008 SP2 werden nicht mehr unterstützt.
- Das Betriebssystem Windows Server 2008 R2 wird ab bMS-Version 2024 R2 nicht mehr unterstützt.
- Die Schnittstelle bMOL wird ab bMS-Version 2025 R1 nicht mehr verfügbar sein.
- Die Schnittstelle httpMOC wird ab bMS-Version 2025 R1 nicht mehr verfügbar sein.
- bMS-Versionen ab 2025 R2 sind mit Oracle Datenbanken nicht mehr kompatibel. Ein Umstieg auf MS-SQL Server oder unsere Cloud Lösung wird empfohlen.

1.7.2 Allgemeine Hinweise

- Ab Version 2023 wird ausschließlich die neue baramundi Lizenzierung unterstützt. Wurde eine vorhandene Installation noch nicht auf die neue Lizenzierung umgestellt, so ist keine gültige Lizenz mehr vorhanden und muss dann nachgetragen werden.
- Das bMS Setup sollte immer lokal, z.B. direkt vom ISO Image gestartet werden. Eine Installation über einen Share kann zu Fehlverhalten führen.

1.7.3 Hinweise zum .NET Framework

- Die benötigen .NET x64 Versionen `Asp.Net Core Framework 6.x` und `NET Core Desktop 6.x` sollten der gleichen Version entsprechen, um Fehlverhalten der baramundi Module zu vermeiden.
- Wird ein .NET Framework deinstalliert und danach neu installiert, so ist ein Neustart des gesamten baramundi Servers notwendig. Obwohl die bMC-Modulansicht keine Fehler zeigt, treten bei dieser Aktion diverse Fehlfunktionen auf.

1.7.4 OS-Install / OS-Cloning

- Hinweis zum bDX-Import von OS-Dateien mit unattend-Dateien: Es wird empfohlen den bDX-Import in diesem Fall direkt auf dem baramundi Server vorzunehmen, damit die unattend-Dateien korrekt im Serververzeichnis unter ..\Shared\Scripts\OS abgelegt werden können.

- Ein Job mit Schritt `Masterimage eines Betriebssystems erstellen` läuft u.U. auf einen Fehler beim Sysprep-Vorgang, wenn er einem Windows 11 Client zugewiesen wurde.

1.7.5 baraDIP

- Die bMS 2024 R1 arbeitet nicht mit älteren baraDIP Versionen. Um Probleme zu vermeiden, können die baraDIP-Dienste noch vor dem Update des bMS auf eine Version 2024 R1 geupdated werden.
- Hinweise zur Verwendung von eigenen Zertifikaten im baraDIP:
    - Über das baraDIP-Config-Tool können bei Bedarf eigene PKI-Zertifikate für den baraDIP konfiguriert werden.
    - Beim Update auf die bMS 2024 R1 werden bestehende PKI-Zertifikatskonfigurationen nicht migriert und müssen daher manuell vorgenommen werden.

1.7.6 Management Center (bMC)

- Unter `bMC - Konfiguration – Domänen` wird in der Detailview statt dem Text "Lokalen Installationsbenutzer verwenden" nur ein "s" angezeigt.
- Ist unter `Managed Software Datensicherheit` eine `Wiederholte schnelle Ermittlung` oder `Wiederholte vollständige Ermittlung` konfiguriert, so sollte der Zeitpunkt so gewählt werden, dass dieser sich nicht mit dem Import der `Managed Software Data Signed`, sowie des anschließenden automatischen Downloads neuer oder geänderter MSW-Dateien kreuzt. Ansonsten kann es zu unerwarteter Anzeige von Hash-Änderungen kommen, welche dann manuell bestätigt werden müssen.
- In der bMC Ansicht `Zuweisungen` sind u.U. OS-Install Jobs kurzzeitig doppelt zu sehen.
- Der Report `List SNMP-Devices` kann in Umgebungen mit einer Oracle Datenbank nicht geöffnet werden.

1.7.7 bRemote

- Die Aufschaltung auf Windows-PE mit `Client – Benutzermenü` Befehl `Connect to PE` läuft u.U. auf einen Authentication-Fehler, wenn bei der bMC-Anmeldung nicht der angemeldete Benutzer verwendet wurde. Gelöst werden kann dies, indem im baramundi RemoteViewer die Anmeldedaten hinterlegt werden.

- Hinweis: Die Unterstützung für Windows XP wurde entfernt.

1.7.8 Remote Desk (AnyDesk)

- Sporadisch erscheint nach dem Start der Aktion `bMC – Client – Fernwartung` eine „AnyDesk crashed“ Meldung.

1.7.9 Mobile Devices

- Durch die Umstellung des Push für Android-Geräte kann es, nach dem Update auf die bMS 2024 R1 bis zu 24h benötigen, bis die Endgeräte wieder Push-Nachrichten erhalten.

- In sehr seltenen Fällen schlägt das Enrollment von Android Enterprise Geräten mit dem Fehler „javax.net.ssl.SSLHandshareException: Der erwartete Fingerabdruck stimmt nicht mit dem vom Server erhaltenen Fingerabdruck überein“ fehl. Dies tritt auf, wenn die automatische Gateway-Zertifikatserneuerung das Zertifikat zwar aktualisiert hat, aber das Gateway noch nicht manuell neu gestartet wurde.

1.7.10 Inventory über SSH für Linux-Geräte

- Bei der Linux Distribution OpenSuse wird die Boottime nicht erfasst.

1.7.11 Inventur

- Die optionale Offline-Inventur verwendet kein PreInvent.bds und unterstützt damit MSW nicht komplett.

- Windows 11 wird von der Softwareinventur als Windows 10 erkannt und kann Anhand der Versionsnummer unterschieden werden.

1.7.12 Windows Agent (bMA)

- Der User Data Collector (UDC.exe) wurde mit bMS-Version 2023 R2 entfernt.

- Variablenwerte für in bD-Skripten verwendete Variablen vom Typ `Passwort` werden nur dann korrekt aufgelöst, wenn der bMA beim Parsen des Skriptes die Variablen erkennen kann. Inhalte für Variablen, wo der Variablenname erst zur Laufzeit des bDS entsteht, werden nicht erkannt und auch nicht mit Werten befüllt.

- Über Profile des Energy Management angewendete Energieoptionen werden unter Windows in den Systemeinstellungen - Energieoptionen unter Umständen nicht korrekt angezeigt. Eine Abfrage der Einstellung auf der Kommandozeile liefert die korrekten Werte und diese werden vom System auch verwendet.

1.7.13 UUID

- Die Umstellung der `Client-Identifizierung` von `MAC` auf `UUID` wird erst empfohlen, wenn ein signierter baramundi UEFI Bootloader verfügbar ist. Bis dahin empfehlen wir weiterhin die Einstellung auf `MAC` zu belassen.

1.7.14 Automation Studio und bD-Script

- Die bDS Aktion `Variablenersetzung in Datei durchführen` ersetzt nur Variablen vom Typ Passwort, die auch in der bDS Datei selbst erkennbar sind.

- Hinweise zu bDS-Dateien ab Version 2022 R2:

    - Beim Öffnen einer bDS-Datei wird auf eine notwendige Konvertierung in das neue Format hingewiesen. Ein konvertiertes Skript kann nur von bMAs der Version 2022 R2 oder höher ausgeführt werden.

    - In Umgebungen mit mehreren baramundi Servern ist darauf zu achten, dass bDSSkripte erst konvertiert werden, wenn alle Server/Clients auf der Version 2022 R2 oder höher sind. Falls eine Konvertierung in das neue Format noch nicht gewünscht ist, kann das Automation Studio der Version 2022 R1 weiterhin verwendet werden.

    - Der bMA ab 2022 R2 kann sowohl das neue bDS-Format, wie auch das bisherige Format ausführen. Eine Konvertierung aller bDS-Skripte ist nicht notwendig.

1.7.15 Windows Agent (bMA) Hinweis für Windows XP

- Die Weiterentwicklung des bMA für Windows XP wurde eingestellt. Sicherheitsupdates für XP sind nicht verfügbar.

- Es ist möglich Windows XP mit dem bMA der Version 2021 R2 weiterhin zu betreiben. Der bMA 2021 R2 ist für diesen Zweck mit der bMS 2022 R1 (und höher) kompatibel.
- Die Features bRemote, OS-Install und automatisches bMA Deployment stehen nicht mehr zur Verfügung. Der bMA muss ggf. manuell installiert werden.
- Hinweis: Windows XP kann nur mit einem veralteten bMA verwendet werden, welcher von baramundi nicht mehr gepflegt wird und bekannte Sicherheitslücken enthält. Es sind keine neuen Sicherheitsupdates für den veralteten bMA verfügbar. Dies ist dem Kunden bekannt. baramundi übernimmt keine Gewährleistung für den sicheren Einsatz von XP und die veraltete bMA-Version. Der Einsatz erfolgt auf eigene Gefahr des Kunden.

2 Release 2023 R2

2.1 baramundi Remote Desk

Mit der baramundi Management Suite 2023 R2 releasen wir eine neue Variante der Fernwartung. Neben dem bisher bekannten baramundi Remote Control gibt es nun die neue Integration von baramundi Remote Desk. In Zusammenarbeit mit unserem Partner AnyDesk Software GmbH haben wir eine direkte Fernwartungsmöglichkeit geschaffen, um aus dem baramundi Management Center heraus auf Endpunkte zuzugreifen.
Zu dem Release 2023 R2 wird es somit möglich sein auf Windows Geräte direkt aus dem baramundi Management Center heraus sicher zuzugreifen, auch wenn sich das Endgerät nicht im LAN oder VPN befindet.

2.1.1 Vorteile durch Partnerschaft

2.1.1.1 Fernwartung aus der Cloud

Mit baramundi Remote Control ist es, bedingt durch die technische Umsetzung mit Windows Remote Support, nicht möglich gewesen, auf Geräte außerhalb des LAN zuzugreifen. Durch den Tunnel des Internetmodus kann der baramundi Management Agent dem Server nun für baramundi Remote Desk die benötigte Session ID zum Aufbau einer Verbindung direkt übertragen.
Durch das dahinterliegende Cloud-Netzwerk von AnyDesk, dem sogenannten „AnyNet“, kann dann direkt eine Verbindung zu den Endpunkten aufgebaut werden, welche sich auch außerhalb des eigenen LAN oder VPNs befinden.

2.1.1.1.1 Rechenzentren

Alle von AnyDesk eingesetzten Rechenzentren sind nach ISO/IEC 27001 zertifiziert und befinden sich in den folgenden Lokationen:

- USA (West-/Ostküste) – Abdeckung ebenso für Teile Lateinamerikas
- Brasilien (Abdeckung der restlichen Teile)
- Spanien
- Frankreich
- Großbritannien
- Niederlande
- Luxemburg
- Deutschland
- Finnland
- Bulgarien
- Türkei
- Israel
- Kasachstan
- Singapur

- China
- Japan
- Australien

Die Verarbeitung personenbezogener Daten erfolgt innerhalb der EU in den Rechenzentren Deutschland und Frankreich.

2.1.1.2 Multi-User-Szenarien

Unser bisheriges Modul baramundi Remote Control hat sich durch die Windows-Remote-Support-Funktion immer auf die Consolen-Session aufgeschaltet und tut dies auch weiterhin. Mit der neuen Lösung baramundi Remote Desk ist es dagegen möglich, sich auch auf unterschiedliche Sessions zu verbinden.

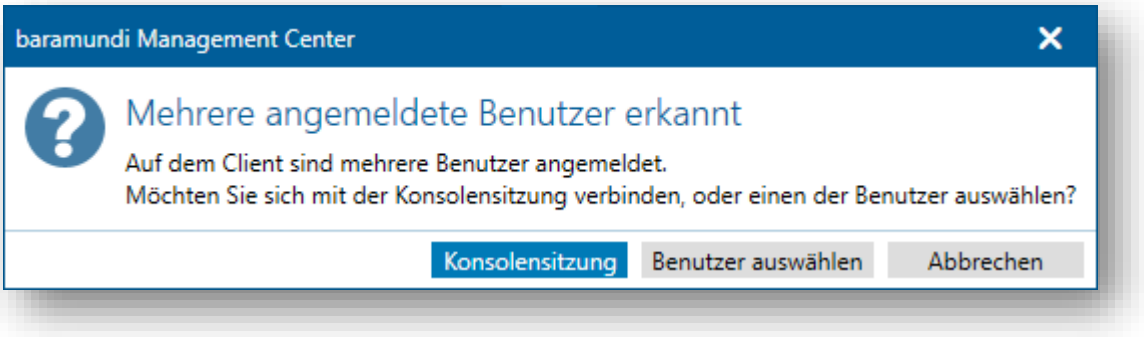


Abbildung 22 - baramundi Remote Desk - Mehrere User-Sessions

2.1.1.3 UAC-Steuerung

Die Windows User Account Control (UAC) verhindert, dass unbefugte Benutzer ohne Erlaubnis des Administrators Änderungen am System vornehmen können.

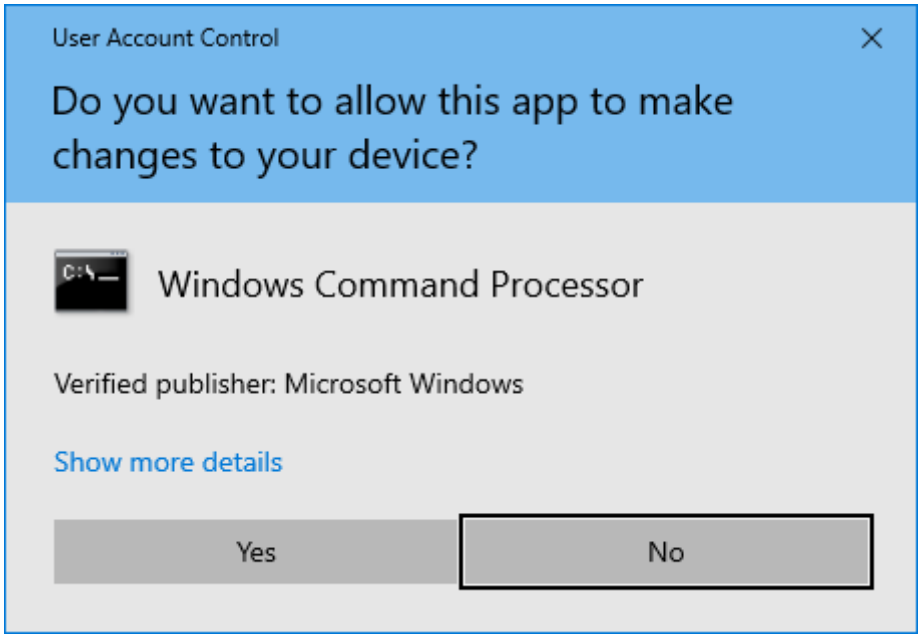


Abbildung 23 - Windows User Account Control

Der Zugriff auf bestimmte administrative Anwendungen ist somit nur zulässig, wenn die Fernwartungslösung mit erweiterten Rechten ausgeführt wird. Bei baramundi Remote Desk ist dies über den Start durch den baramundi Management Agent möglich.
Das bedeutet, dass Prompts und Einstellungen „hinter“ der UAC somit mit baramundi Remote Desk gesteuert werden können.

2.1.1.4 Tastatur und Hotkeys

Tastenkombinationen werden durch die Session an das Zielgerät durchgereicht, das heißt, es kann wie gewohnt mit beispielsweise STRG+C und STRG+V gearbeitet werden oder auch der Taskmanager mit der Kombination STRG+Shift+ESC geöffnet werden.

Für internationale Nutzer:innen, die eine Verbindung von einem Sprachraum in einen anderen herstellen, bietet baramundi Remote Desk eine Funktion zur Übersetzung der Tastaturbelegung. So kann beispielsweise ein Benutzer in Polen, der eine polnische Tastaturbelegung verwendet, eine Verbindung zu einem Rechner in Frankreich herstellen, der eine französische Tastaturbelegung verwendet, und unabhängig von den unterschiedlichen Tastaturbelegungen arbeiten. In den meisten Fällen wird baramundi Remote Desk den besten Modus für den Benutzer wählen. In einigen speziellen Fällen kann es erforderlich sein, den Tastaturübersetzungsmodus manuell zu wählen.

2.1.1.5 Dateitransfer

baramundi Remote Desk bietet Optionen zur Übertragung von Dateien zwischen dem lokalen und dem Remote-Endgerät. Dies kann über eine "Dateimanager"-Sitzung oder über "Dateiübertragung" innerhalb einer Remote-Control-Sitzung erfolgen.

Dateimanager

Die spezielle Dateimanager-Funktion ist verfügbar auf Windows. Um eine spezielle Dateimanager-Sitzung zu starten, klicken Sie einfach auf das Symbol.

Um den Dateimanager während einer interaktiven Remote-Sitzung zu verwenden, starten Sie ihn einfach über die Toolbar. Sofern man sich auf eine aktive Benutzer-Session schaltet, muss der Dateitransfer vom Benutzer vorab genehmigt werden, sodass nicht ohne dessen Wissen Dateien im Hintergrund transferiert werden.

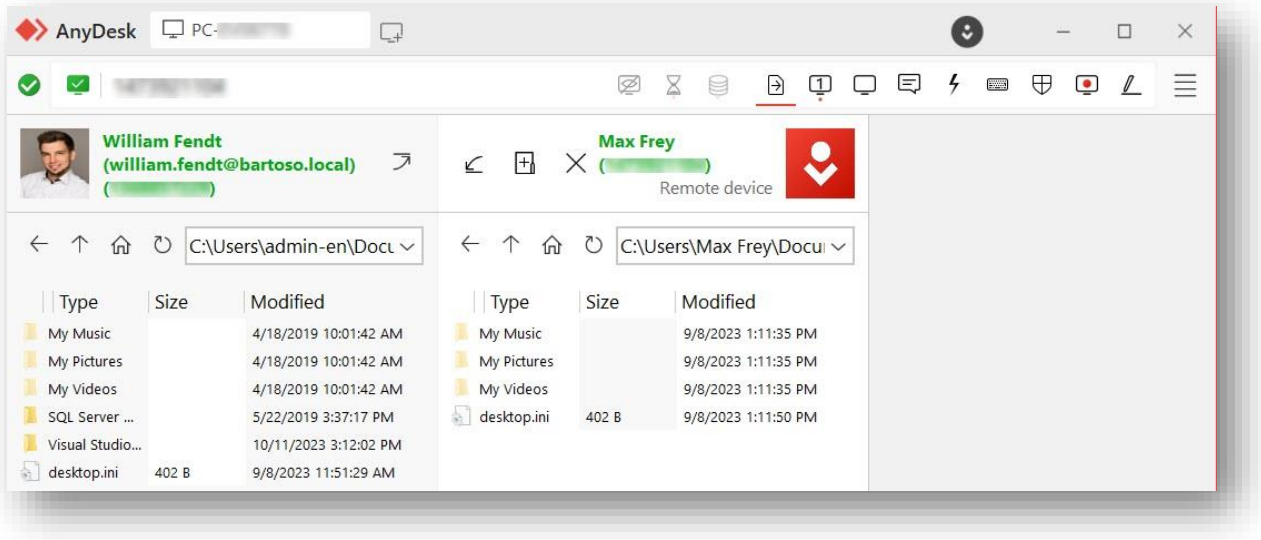


Abbildung 24 - baramundi Remote Desk - Dateimanager

Dateiübertragung

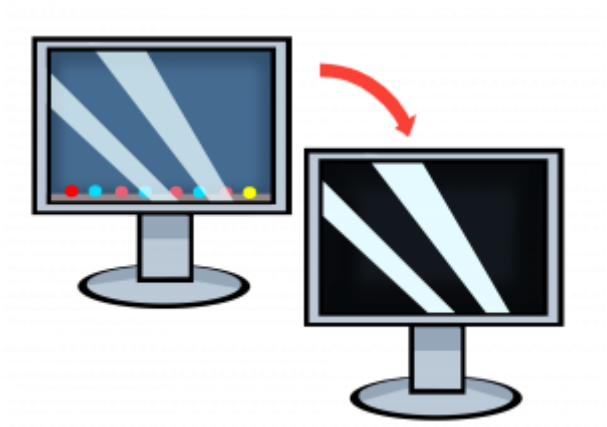
AnyDesk bietet die Möglichkeit, die Zwischenablagen zwischen dem lokalen und dem Remote-Endgerät zu synchronisieren, was sowohl für Texte als auch für Dateien gelten kann.
Diese Funktion wird über die "Kopieren & Einfügen"-Funktionen aller gängigen Plattformen angeboten.

2.1.1.6 Privacy Mode

Der "Privatsphäremodus" oder privater Modus ist eine Funktion, mit der Sie den Inhalt einer Sitzung verbergen können, indem Sie die Remote-Anzeige deaktivieren.

Wenn der "Privatsphäremodus" oder private Modus aktiviert ist, wird der Bildschirminhalt vor allen Personen verborgen, die physischen Zugriff auf das Remote-Gerät haben.

Darüber hinaus werden bei aktiviertem privaten Modus auch die Eingabe und der Ton von der Remote-Seite blockiert, bis entweder die Sitzung beendet oder der private Modus manuell deaktiviert wird.



Der Privatsphäremodus verbirgt jedoch keine Aktionen des Betriebssystems oder einen Verlauf auf dem lokalen oder Remote-Gerät.

Damit der private Modus aktiviert werden kann, ist die Zustimmung der Clients auf beiden Seiten der Sitzung erforderlich.

2.1.1.7 Chatfunktion

baramundi Remote Desk bietet die Möglichkeit, Nachrichten zwischen zwei Endpunkten sowohl während einer Verbindungsanfrage als auch während einer Sitzung zu versenden.

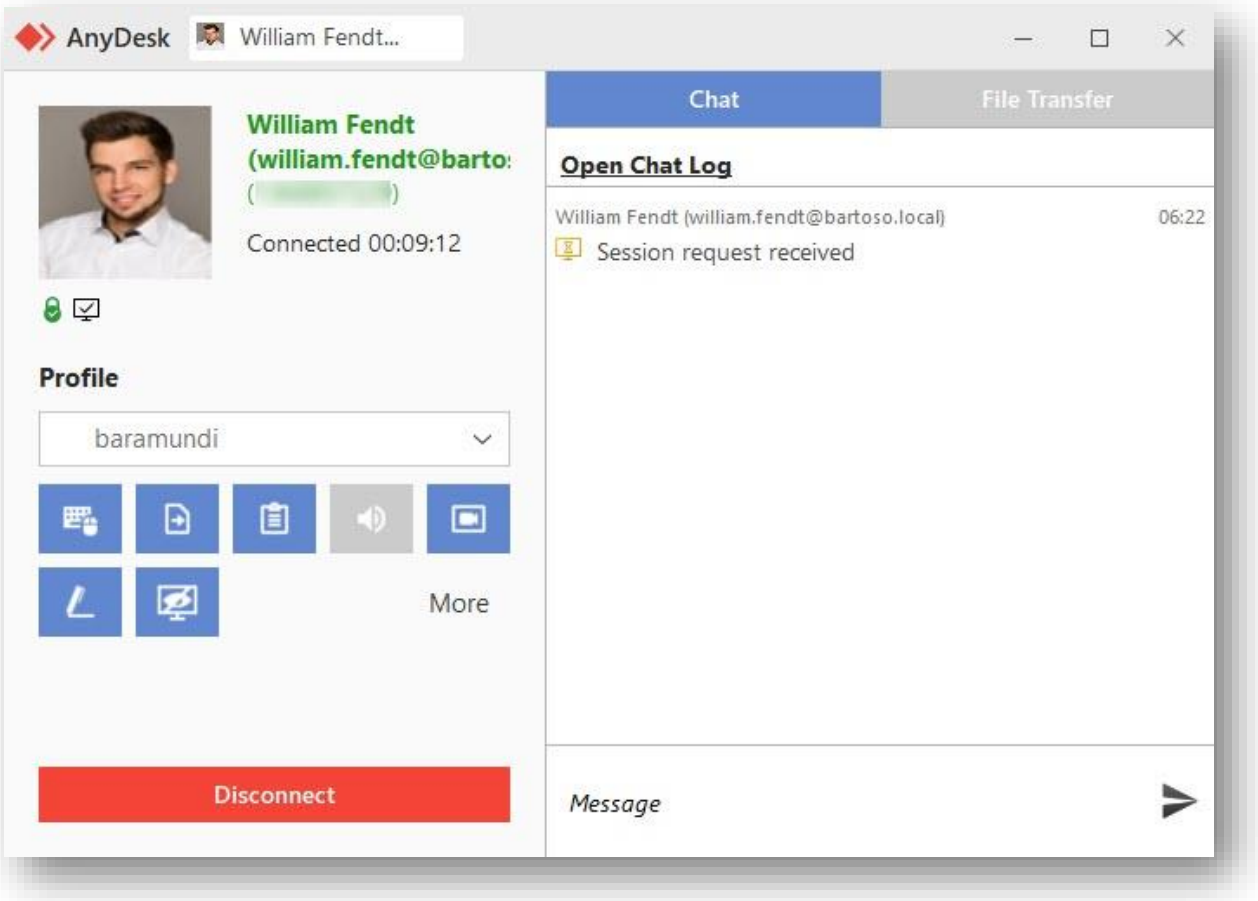


Abbildung 25 - baramundi Remote Desk - Chat Client

AnyDesk speichert auch einen Verlauf der Chatnachrichten vom und zum Client. Standardmäßig werden die Chatprotokolle an folgendem Ort gespeichert: *%appdata%\AnyDesk\ad_<prefix>\chat*

Die Chatverläufe sind nach der AnyDesk-ID des verbundenen Endgeräts geordnet. Mehrere Chats zwischen denselben IDs in verschiedenen Sitzungen werden in einer Datei zusammengefasst.

2.1.2 Vorteile der baramundi-Integration

Durch das im Einsatz befindliche baramundi Management Center wie auch den bereits auf dem System installierten bMA ergeben sich einige Vorteile für die Remote-Verbindungen.

2.1.2.1 Direkt ohne weitere Installation nutzbar

Durch die automatische Verteilung des Clients über unseren bMA ist keine zusätzliche Verteilung notwendig. In anderen Worten heißt dies, um eine Remote-Session aufzubauen, ist nur ein Update des baramundi Management Agents auf die Version 2023 R2 notwendig. Ab dann kann die Funktion direkt aus dem Management Center heraus verwendet werden.

2.1.2.2 „Bekannte" Personal Settings

Durch die Verwendung unserer bisherigen Schnittstellen ist es ohne weiteres Zutun möglich, dass die bisherigen persönlichen Einstellungen für baramundi Remote Control auch für die neue Lösung baramundi Remote Desk übernommen werden. Hierbei verwendet baramundi Remote Desk den Anzeigenamen wie auch das User-Bild, welches bereits hinterlegt wurde.

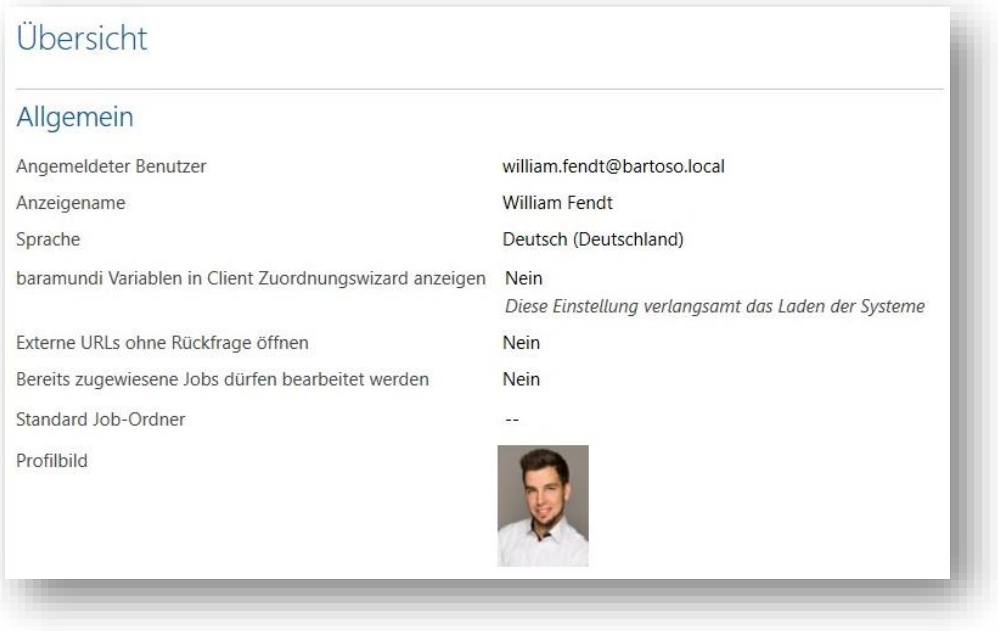


Abbildung 26 - baramundi Remote Desk - Persönliche Einstellungen

Ebenso ist es für den Benutzer am Zielssystem ein gewohntes Bild. Die initiale Kommunikation erfolgt hierbei über unseren TrayNotifier und liefert ein bekanntes und vertrautes Layout für den User zur Bestätigung einer Aufschaltung.

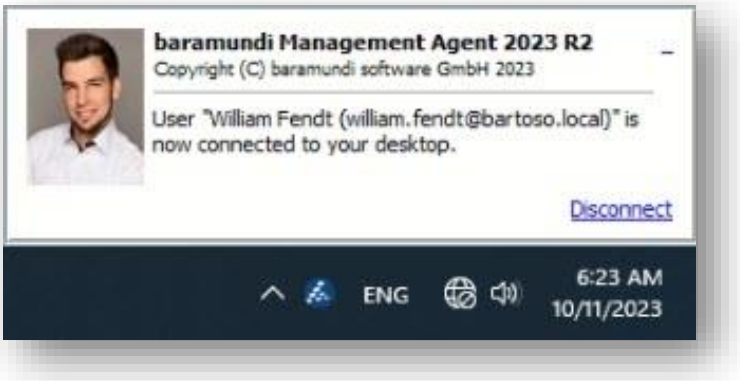


Abbildung 27 - baramundi Remote Desk - Tray Notification

2.1.2.3 Logged on / Not logged on – Differenzierung durch bMA

Durch eine bereits bestehende Kommunikation zwischen dem baramundi Server und dem baramundi Management Agent kann automatisch und flexibler die Session initiiert werden. So können eine User-Session oder gar bestimmte User-Sessions (siehe 2.1.1.2) verwendet werden. Sofern kein User am System angemeldet ist, kann die Anmeldung durch unseren bMA erfolgen und selbige dann verwendet werden. Bei Beendigung erfolgt der Log-off automatisiert, sodass keine Session versehentlich offen bleibt.

2.1.2.4 AnyDesk läuft nur nach Start von bMA

Unser baramundi Management Agent funktioniert im Falle von baramundi Remote Desk wie eine Art Gateway: Die eigentliche Anwendung zum Aufbau einer Fernwartungssitzung wird erst vom bMA gestartet, wenn er diesen Befehl vom Server erhält. Somit ist es trotz einer Erreichbarkeit der Endgeräte im Internet nicht möglich, allein durch die Session ID oder gar nur durch „ID-Guessing“ auf ein Zielsystem zu gelangen, welches mit baramundi Remote Desk arbeitet.

Dies ist ein Sicherheitsaspekt, dadurch dass das Zeitfenster für eventuelle Anfragen enorm verkleinert wird und zwar nur nach Aufforderung durch den legitimierten bMA.

2.1.2.5 Whitelisting durch bMC und bMA

Standardmäßig nimmt unsere baramundi Remote Desk Lösung (selbst wenn diese gestartet worden wäre; siehe 2.1.2.4) keinerlei Anfragen an und lässt nur Sessions auf der Whitelist zu. Genau diese wird vor Session-Aufbau von unserem baramundi Management Agent mit der Session-ID des Quellsystems beschrieben. Somit wird ein zusätzlicher Sicherheitsschritt eingebaut, dass keine fremden IDs Zugriff auf diese baramundi Remote Desk Installation auf dem Endgerät haben.

2.2 Inventory über SSH für Linux-Geräte

baramundi weitet die Inventur der Netzwerkgeräte aus. Ab dem kommenden Release werden verschiedene, aktuelle Linux-Distributionen über die neue Inventur unterstützt (z.B. Red Hat, Debian, Ubuntu, OpenSUSE, Raspberry Pi OS).

Um die Inventur zu starten, müssen die Geräte der bMS vorab manuell oder automatisiert mittels Netzwerk-Scan bekannt gemacht werden. Anschließend können sie per Job über eine SSH-Verbindung inventarisiert werden.

Durch die Verwendung von SSH wird auf dem Netzwerkgerät kein Agent benötigt. Gerade in produktionsnahen Umgebungen oder allgemein in der OT ist das ein entscheidender Vorteil, da hier Agenten oft nicht ohne Weiteres installiert werden können. Die SSH-Authentifizierung kann dabei mittels Benutzername und Passwort oder alternativ über SSH-Keys erfolgen.

Der folgende Screenshot zeigt beispielhaft das Ergebnis eines Inventur-Jobs eines Linux-Devices:

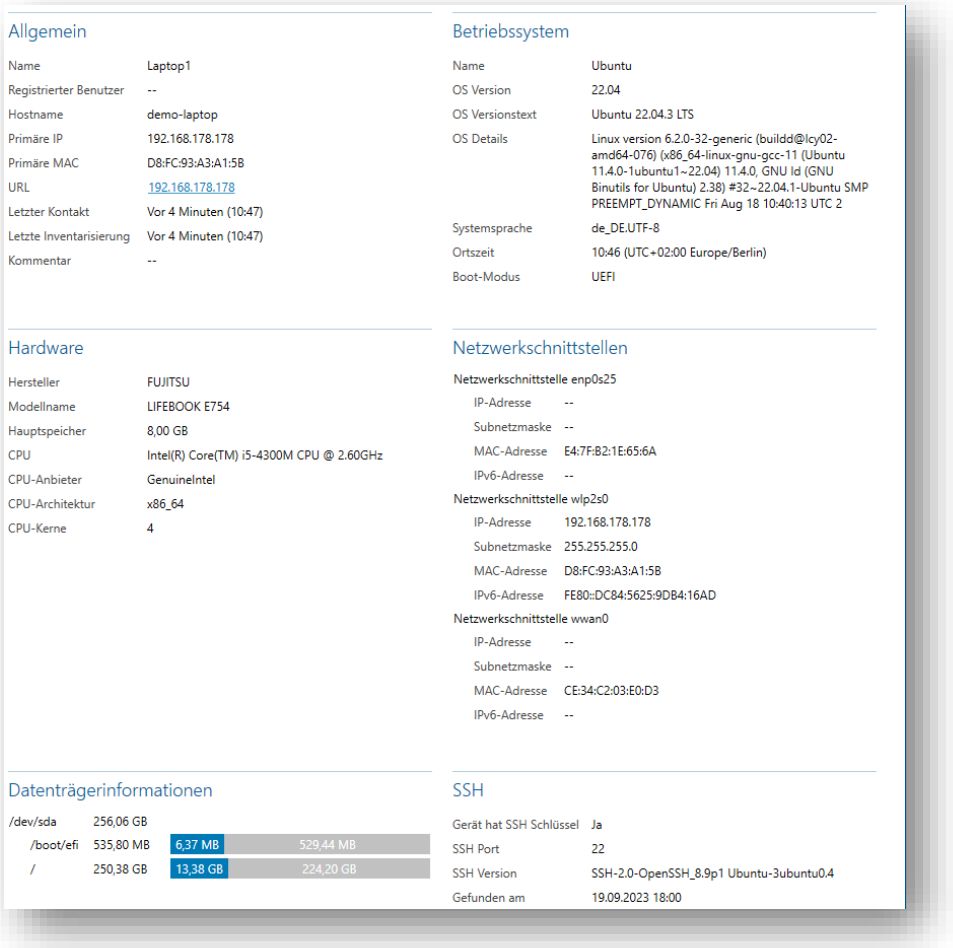


Abbildung 28 – Ergebnis eines SSH Inventurjobs eines Linux-Gerätes

Selbstverständlich können die dadurch neu gewonnenen Informationen in UDGs genutzt und über bConnect ausgelesen werden.

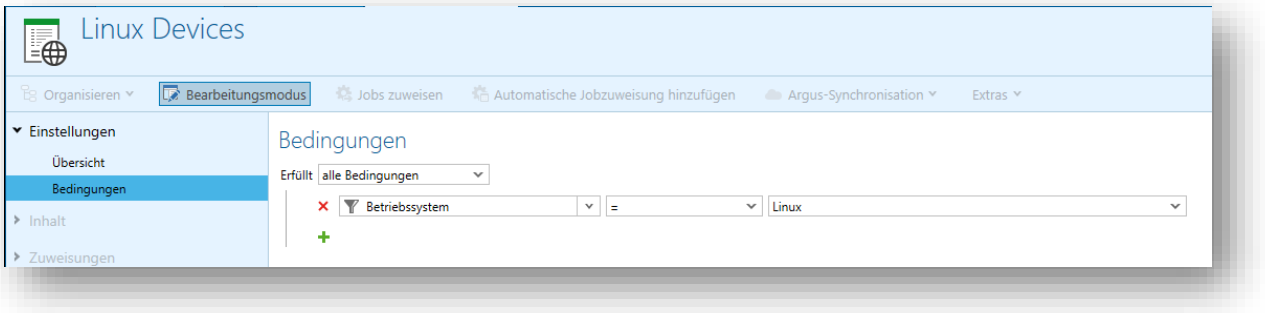


Abbildung 29 – zeigt eine UDG mit aktivem Filter auf Betriebssystem=Linux

2.3 Single Sign-on im Kiosk

Mit der Einführung des neuen Kiosks auf Basis einer modernen WebApp im Jahre 2018 wurde neben der Bereitstellung von Jobs auf Endpoint-Ebene auch die Möglichkeit geschaffen, Jobs gezielt für einzelne Benutzer- und Benutzergruppen bereitzustellen.
Hierfür ist es erforderlich, dass Anwender:innen sich korrekt am Kiosk anmelden – je nach Vorgaben des Unternehmens, zu z. B. Benutzernamen, kann das zu einer Hürde für Anwender:innen werden – die Anmeldung ist zu kompliziert, die Usersicht wird nicht verwendet.

Mit der kommenden Version der baramundi Management Suite wird sich dieser Umstand ändern!

Wird der Kiosk per URL in einem unterstützten Browser geöffnet, werden die Anmeldedaten durchgereicht und der User entsprechend im Kiosk angemeldet. Stehen Jobs für diesen User bereit, kann er sie auf die für ihn registrierten Geräte zuweisen.

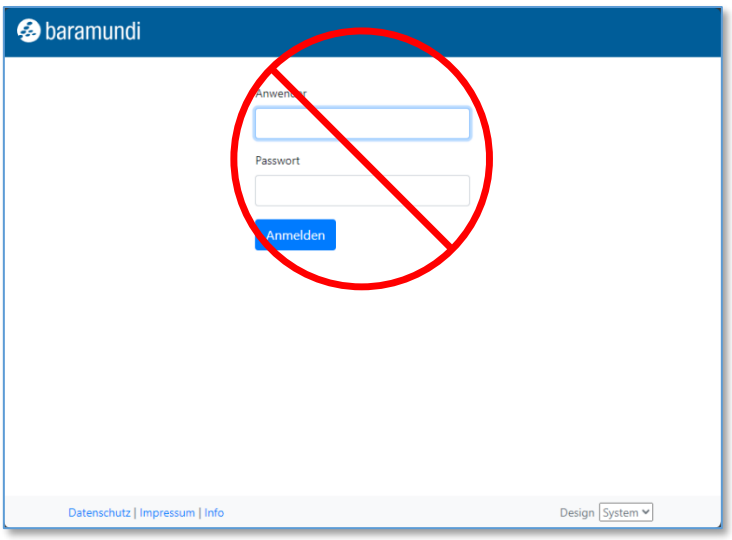


Abbildung 30 - Eine manuelle Anmeldung ist nun nicht mehr nötig (Symbolbild)

Sofern der Kiosk über das Symbol im Tray gestartet wird, muss zuerst auf die Schaltfläche „Anmelden“ geklickt werden – auch hier erfolgt nun eine automatische Anmeldung.

2.4 Mobile Devices

2.4.1 Android Zero-Touch

Die automatische Aufnahme von neuen (oder zurückgesetzten) Endpoints ist eine der wichtigsten Funktionen einer Endpoint-Management-Lösung – nicht nur im Bereich der mobilen Endgeräte. Nach der Unterstützung für Apple-Geräte per DEP und Windows-Geräte per Autopilot ist nun auch die Unterstützung für Android-Geräte per Zero-Touch mit an Bord.

Mit Android Zero-Touch werden Geräte bei der Inbetriebnahme automatisch mit der bMS als Managementsystem verbunden und sofort mit den festgelegten Einstellungen und Apps versorgt.

2.4.1.1 Ablauf

Über ein von Google bereitgestelltes Portal kann Zero-Touch für das Unternehmen eingerichtet werden. Nach erfolgreicher Einrichtung können Neugeräte vom unterstützenden Lieferanten eingetragen werden und sind umgehend sichtbar.

Meldet sich nun bei der Inbetriebnahme das Gerät bei Google, wird es an den baramundi Management Server weitergeleitet und startet dort mit dem Enrollment. Sobald dieser Prozess gestartet wurde, ist das Gerät in der baramundi Management Console sichtbar und kann mit dem gewünschten Enrollment-Profil versorgt werden – selbstverständlich kann hier auch ein Enrollment-Profil als Standard vordefiniert werden. Als Profiltypen stehen das „Vollständig verwaltete Gerät“ (Fully Managed Device) und das „Zweckbestimmte Gerät“ (Dedicated Device) zur Verfügung.

2.4.1.2 Zero-Touch in der bMS

Um Zero-Touch in der bMS nutzen zu können, muss einmalig eine Verbindung zwischen bMS und der Zero-Touch-Infrastruktur hergestellt werden. Innerhalb der bMS kann dann noch bestimmt werden, ob Geräte (nach erfolgreicher Inbetriebnahme) erneut enrollt werden dürfen, z. B. nach einem Reset auf Werkseinstellungen. Ebenso kann festgelegt werden, dass nur regelkonforme Geräte akzeptiert werden. Selbstverständlich kann auch die standardmäßige Gruppe innerhalb der „Logischen Gruppierung“ und der Kreis der erlaubten Benutzer festgelegt werden.

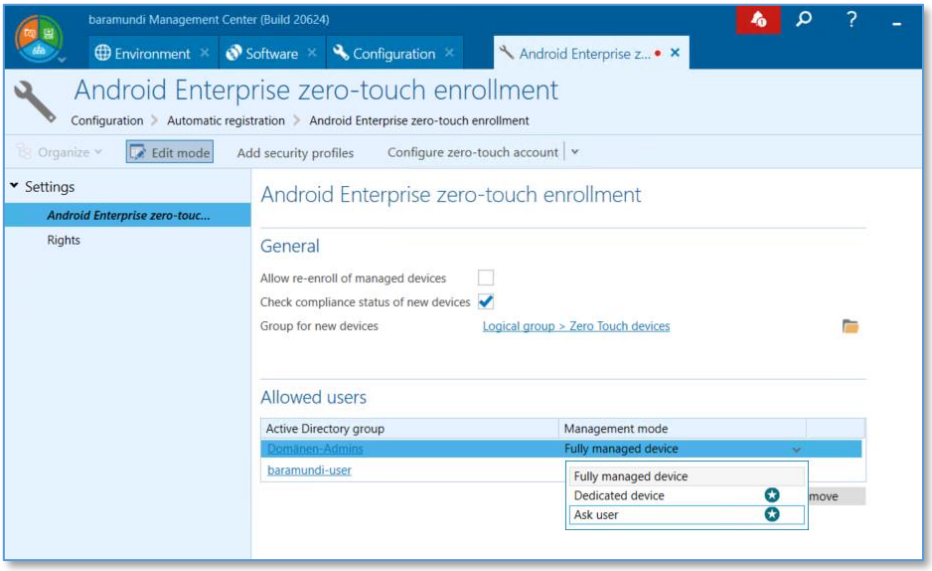


Abbildung 31 - Konfigurationsseite für Zero-Touch

Über die Benutzergruppe oder den Benutzernamen kann vorgegeben werden, ob das Gerät als „Vollständig verwaltet“ oder „Zweckbestimmt“ eingerichtet wird. Sofern vom Admin freigegeben, kann auch der User am Gerät den Modus selbst wählen – das ist so bisher nur mit der baramundi Management Suite möglich!

2.4.2 Weitere Verbesserungen

2.4.2.1 Standortgenauigkeit verbessern

Der Jobschritt “Befehl ausführen” für Android Enterprise wurde um das Kommando „Improve Location Accuracy“ erweitert.

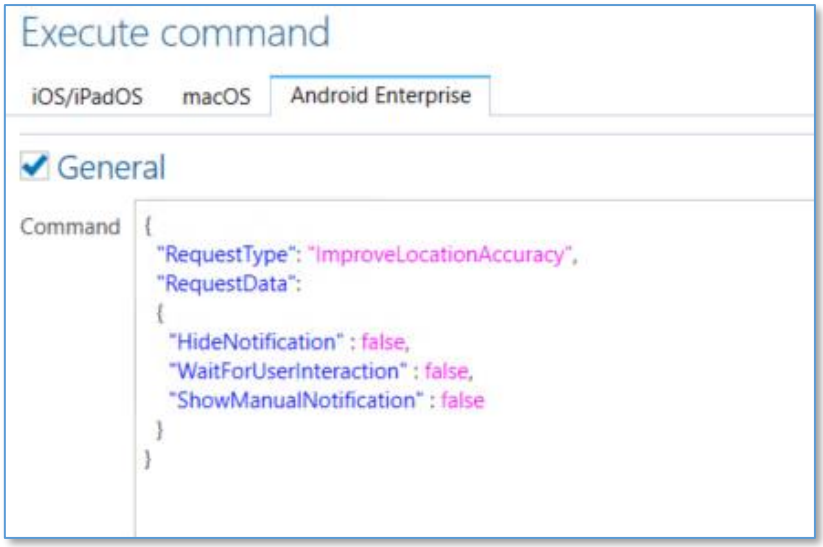


Abbildung 32 - Konfiguration des Kommandos zur Standortgenauigkeitsverbesserung

Dieser Befehl ruft die Standortgenauigkeitsverbesserungsabfrage für den User auf, um eine genauere Erfassung des Standorts zu ermöglichen.

2.4.2.2 App-Start per Activity

Im Template für ein zweckbestimmtes Android-Gerät können nun Activities für den direkten Start einer App angegeben werden. Somit ist es möglich, eine App zu starten, die nicht direkt per Launcher/Homescreen aufrufbar ist (z. B. einige System-Apps).

2.5 Universelle Dynamische Gruppen

2.5.1 Neue Bedingungen für UDGs

Auch in dieser Version haben wir neue Eigenschaften für die Filterung in UDGs hinzugefügt. Neben der „normalen“ Eigenschaft des Apple Silicon Chips haben wir die Querreferenz auf andere UDGs implementiert.

.

2.5.2 UDG in UDG

Oft gibt es eine bestimmte Bedingung, welche häufiger wiederverwendet werden muss. Um diese, oder dieses Set von Bedingungen, weiter verwenden zu können, kann nun mit der „Gruppenzugehörigkeit“ einfach auf eine bestehende Gruppe referenziert werden.

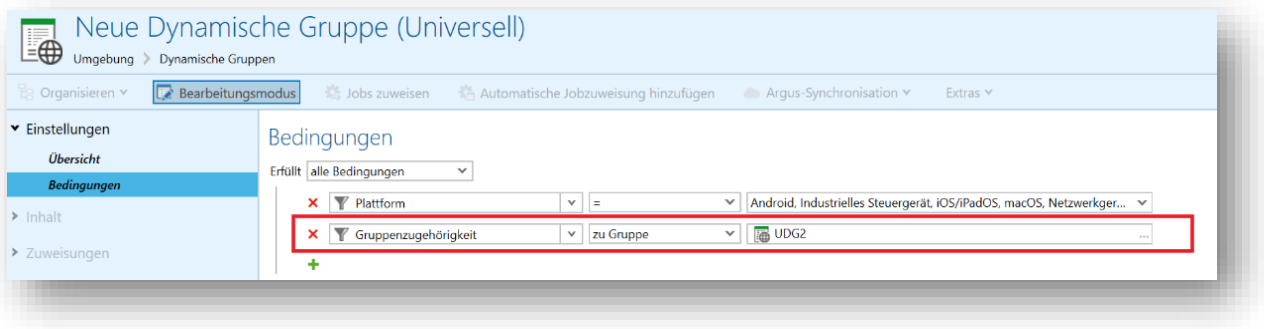


Abbildung 33 - UDG Gruppenzugehörigkeit

Auch beim Fehlerhandling wird man durch die UDGs unterstützt. Denn es kann hierbei vorkommen, dass man innerhalb einer UDG auf eine bestehende verweist, welche wiederum einen Kreisverweis erzeugen würde. Dies wird mit den neuen UDGs direkt beim Speichern abgefangen.

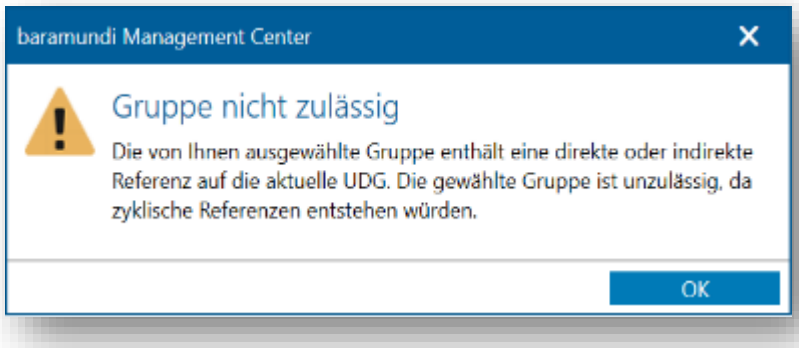


Abbildung 34 - UDG Kreisverweis

Ebenso wird das baramundi Management Center eine Warnung anzeigen, sofern eine UDG bearbeitet wird, welche Einfluss auf eine referenzierende UDG besitzt, die wiederum eine „Automatische Jobzuweisung“ hinterlegt hat.

2.5.3 Apple Silicon

Für macOS Geräte gab es die Anforderung diese nach dem verbauten Apple Silicon Chip zu filtern. Mit unseren Universellen Dynamischen Gruppen ist dies nun eine neue abfragbare Bedingung.

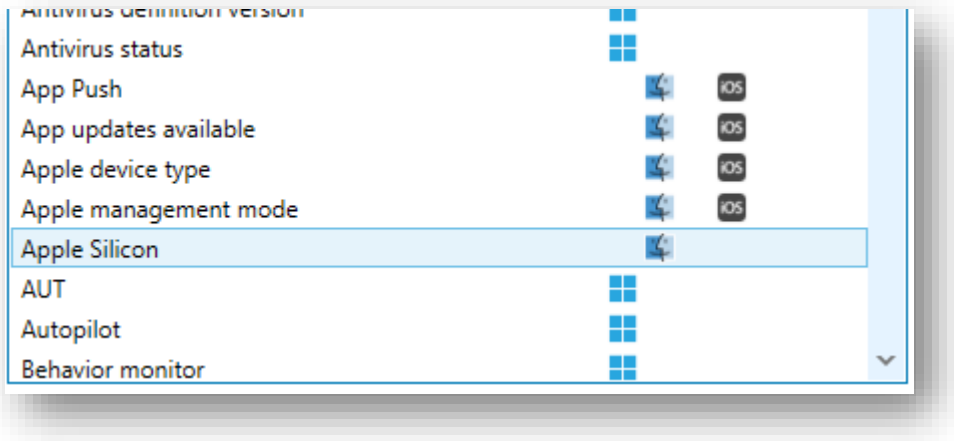


Abbildung 35 - UDG Bedingungen

Die Eigenschaft ist somit einfach als boolesches Feld (Ja/Nein) in UDGs verwendbar und kann somit als Filterung und für automatische Zuweisungen verwendet werden.

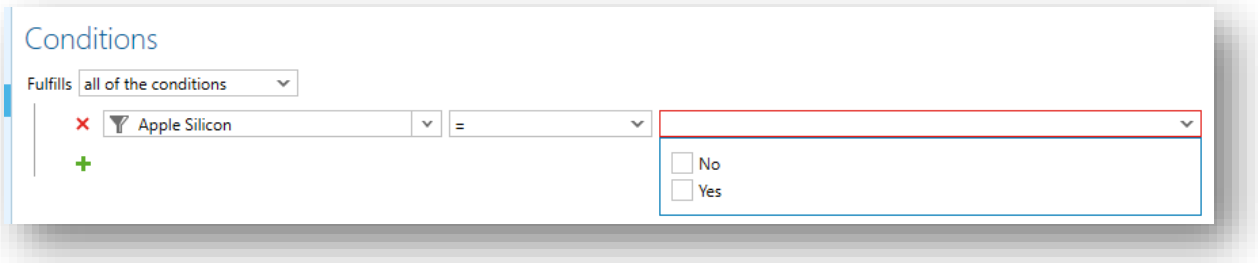


Abbildung 36 - UDG Apple Silicon

2.6 Network Devices

2.6.1 Skriptausführung über SSH

Als Bestandteil der Verwaltung von jeglichem Netzwerk Gerät ist es von Vorteil diesen mithilfe der baramundi Joblogik auch Skriptausführungen zuzuweisen. Dies erfolgt einfach als neuer Jobstep im neuen „Job für OT oder Netzwerkgeräte“.

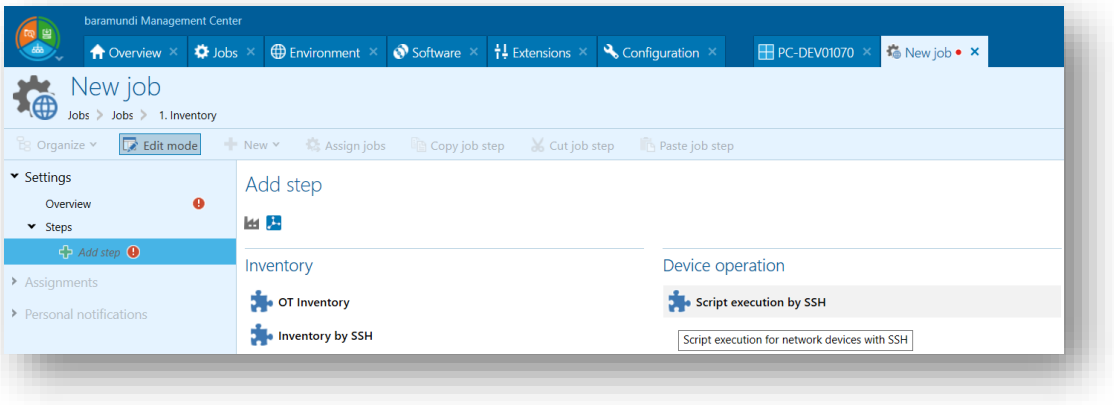


Abbildung 37 - Neuer Jobstep

Hier hat man dann direkt die Möglichkeit auf ein Skript auf dem DIP zu verweisen, welches für das jeweilig zugewiesene Gerät gestartet werden soll.

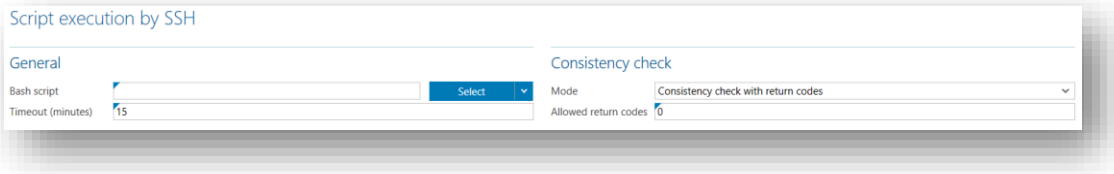


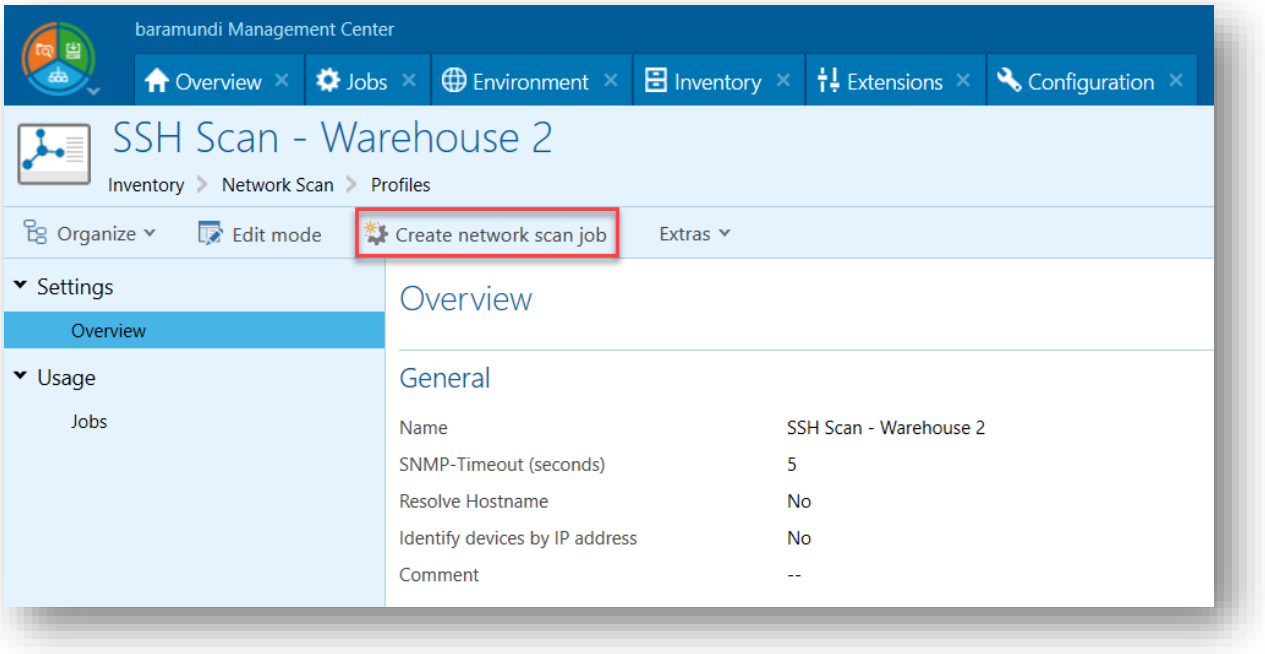
Abbildung 38 - Skriptausführung via SSH

Beispiel Skript:

```
#!/bin/bash
# Choose port between 1024 and 65535
$SSHPORT = 1025
sed -i -e "/Port /c\Port $SSHPORT" /etc/ssh/sshd_config
echo -e "Restarting SSH in 5 seconds. Please wait.\n"
sleep 5
# Restart SSH service
service sshd restart
echo -e "The SSH port has been changed to $SSHPORT. Please login using that port to test BEFORE ending this session.\n"
exit 0
```

2.6.2 Netzwerk-Scan-Profile

Das Arbeiten mit Netzwerk-Scan-Profilen wurde in dieser Version erweitert. Zum einen wurde das Erstellen von Jobs für Scans vereinfacht, indem direkt am Netzwerk-Scan-Profil die Option im Menü hinterlegt wurde, einen Job mit diesem Profil zu erstellen.



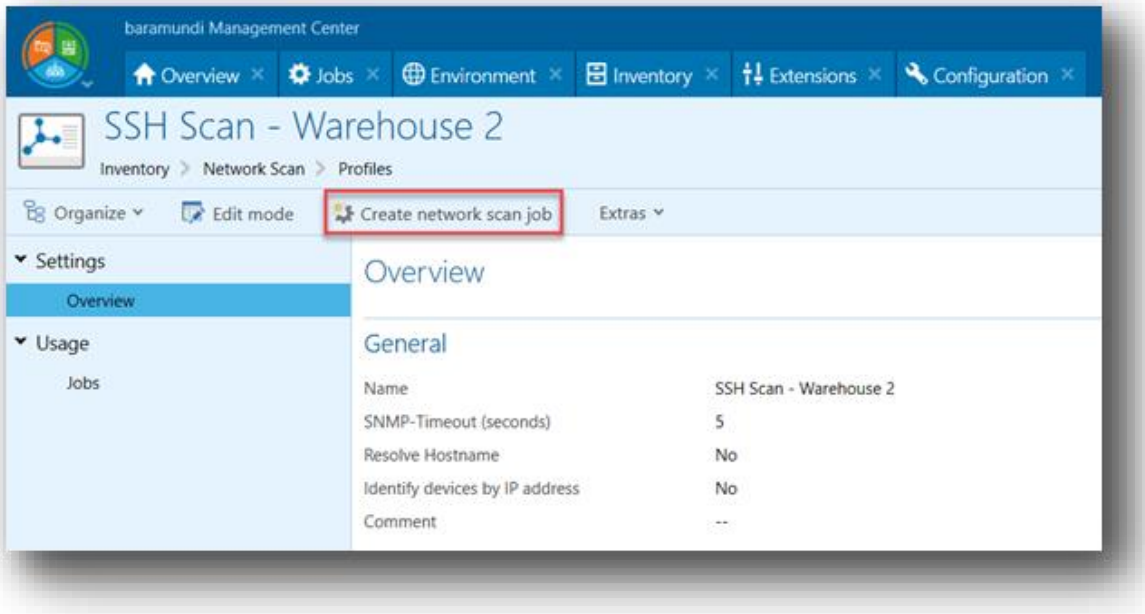


Abbildung 39 - Netzwerk-Scan-Profil - Netzwerk-Scan-Profil - Neuen Job anlegen

Zum anderen kam beim Netzwerk-Scan-Profil die neue Option hinzu, dass unter Verwendung dieses Profils kein Abgleich mit weiteren Endgeräten außerhalb der Zielgruppe stattfinden soll. Dies ist erforderlich, sofern an mehreren Standorten beispielsweise Netzwerkgeräte mit den gleichen Identifizierungsmerkmalen existieren (Name und IP-Adresse).

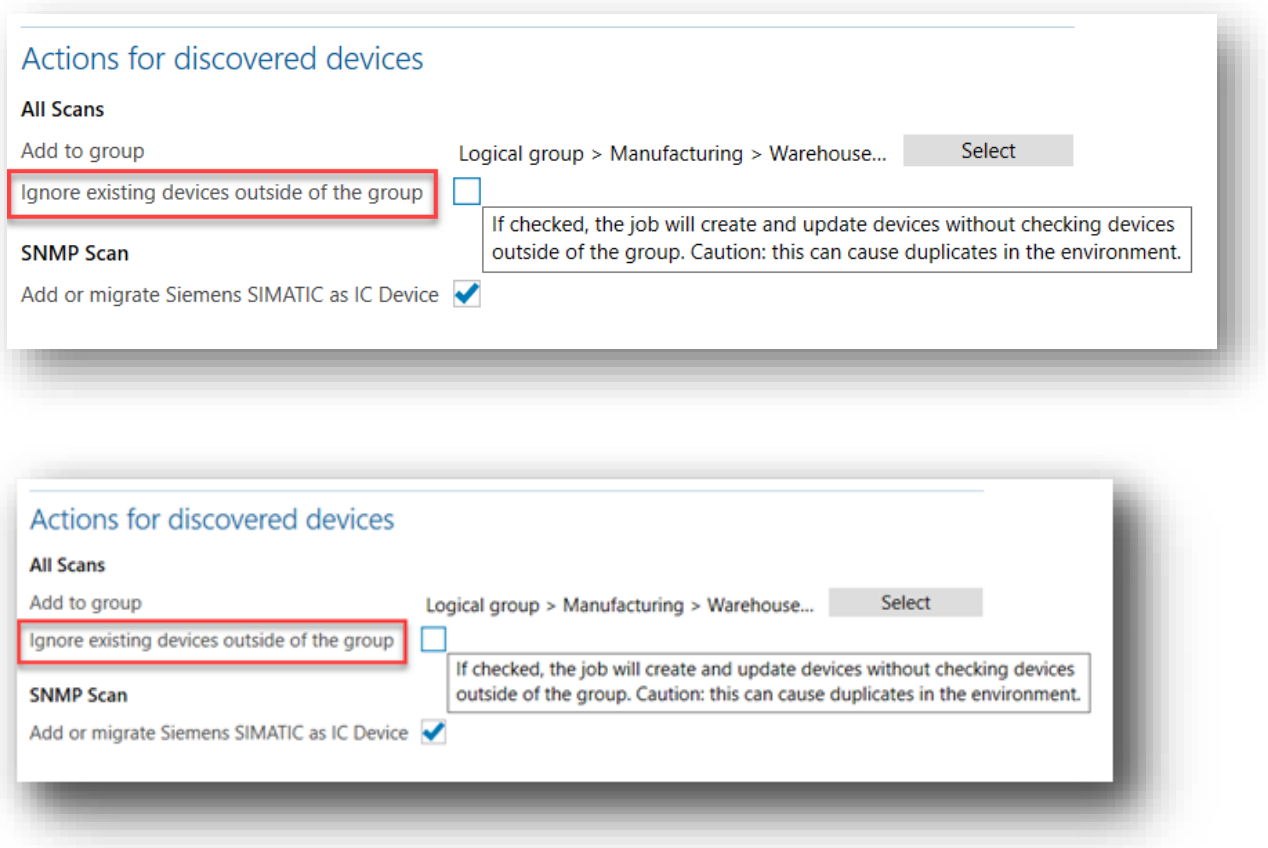


Abbildung 40 - Netzwerk Scan Profil - Andere Geräte ignorieren

2.7 Weiterentwicklungen in Argus Experience

Plötzliche, ohne Vorwarnung auftretende IT-Probleme sind immer möglich, aber die große Mehrzahl kündigen sich mehr oder weniger subtil an. Diese IT-Probleme sorgen für viel Frust bei den End Usern und rauben der IT-Administration viel Zeit. Mit baramundi Argus Experience (bEX) lassen sich diese Signale frühzeitig erkennen, richtig interpretieren und entsprechende Gegenmaßnahmen einleiten.

2.7.1 Langsame Computerstartzeiten

Eine der häufigsten User-Beschwerden ist eine langsame Boot-Geschwindigkeit. Das Verkürzen dieser Rüstzeit bietet aufgrund ihrer Allgegenwärtigkeit enormes Potenzial, um die Belegschaft schneller in einen produktiven Zustand zu versetzen.
Doch es ist nicht nur die Ladezeit selbst, die Auffälligkeiten zeigt, sondern auch folgende Aspekte können mit Argus Experience in die Analyse einfließen:

- Sind einzelne oder mehrere Endgeräte besonders auffällig?
- Gibt es bestimmte Zeiträume, in denen das Hochfahren außerordentlich lange dauert?

- Welche Soft- und Hardwarekomponenten sind bei diesen Endgeräten zu finden?
- Welche Phasen der Startzeiten sind besonders langsam und damit auffällig?

Diese Elemente können mit bEX erfasst und ausgewertet werden. Das ermöglicht IT-Admins, z. B. durch Softwareupdates, Betriebssystemupgrades oder Hardwaretausch, diese Flaschenhälse unternehmensweit zu überwinden.

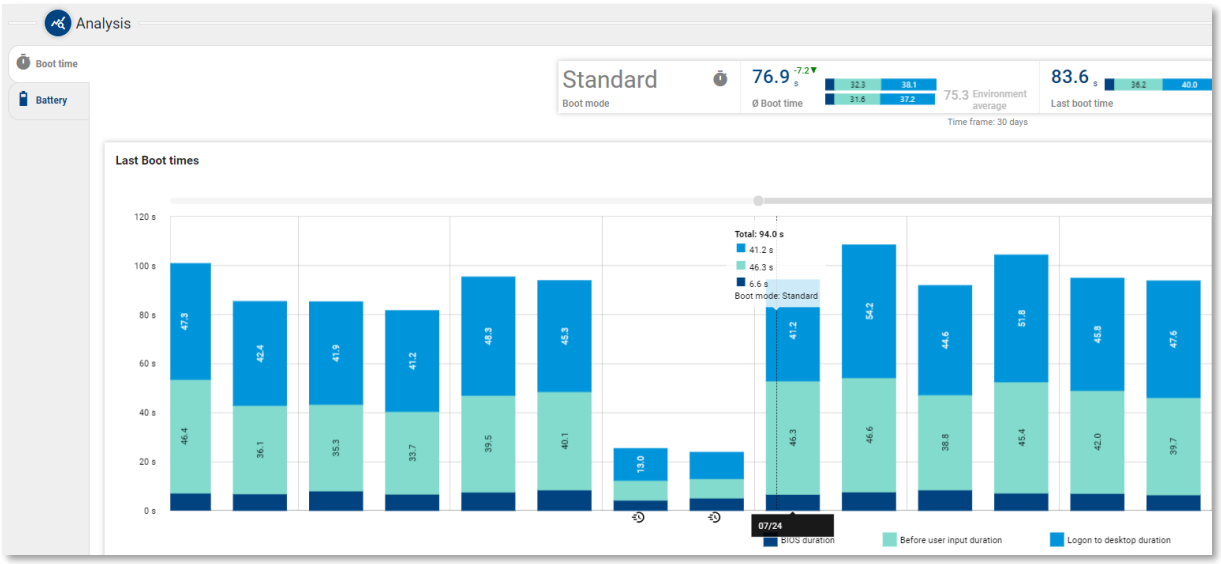


Abbildung 41 - Detaillierte Startzeiten eines Endgerätes

2.7.2 Akku-Verschleiß im Laptop

Häufiges mobiles Arbeiten setzt die in Laptops verbauten Akkus großem Stress aus. Die Folge ist mit der Zeit abnehmende Kapazität, bis plötzlich nur wenige Minuten Leistung verbleiben. Dabei ist für die User häufig gar nicht genau ersichtlich, wie sehr der Akku bereits abgebaut hat – bis der Rechner dann in einem kritischen Moment abschalten muss.

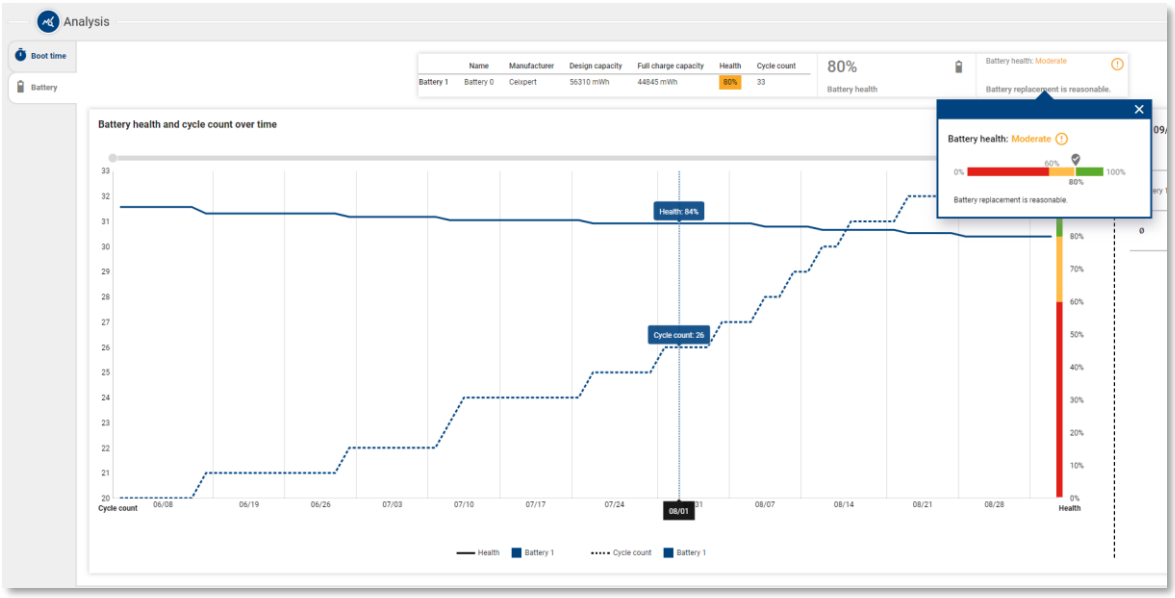


Abbildung 42 - Kritische Akku-Kapazitäten eines Endgerätes im Fokus

Dieses Szenario lässt sich durch baramundi Argus Experience effektiv vermeiden: Die entsprechenden Leistungszahlen können über die Zeit erfasst und ausgewertet werden. Die IT kann so allen Mitarbeitern schon einen neuen Akku bereitstellen, bevor das Problem akut wird.

2.7.3 Programmabstürze

Die Interaktion verschiedener Programmversionen ist häufig der Auslöser für weiterreichende Probleme. Ein Beispiel dafür ist Microsoft PowerPoint. In der Vergangenheit haben Entwickler den Funktionsumfang zwischen den verschiedenen Versionen immer wieder leicht verändert. Für die eine Version erstellte Präsentationen funktionieren dann nicht mehr oder nicht richtig auf Geräten mit einem anderen Softwareversionsstand. Für die User ist es ein Rätsel, warum die gleiche Präsentation bei einem Rechner funktioniert, bei einem anderen aber nicht.

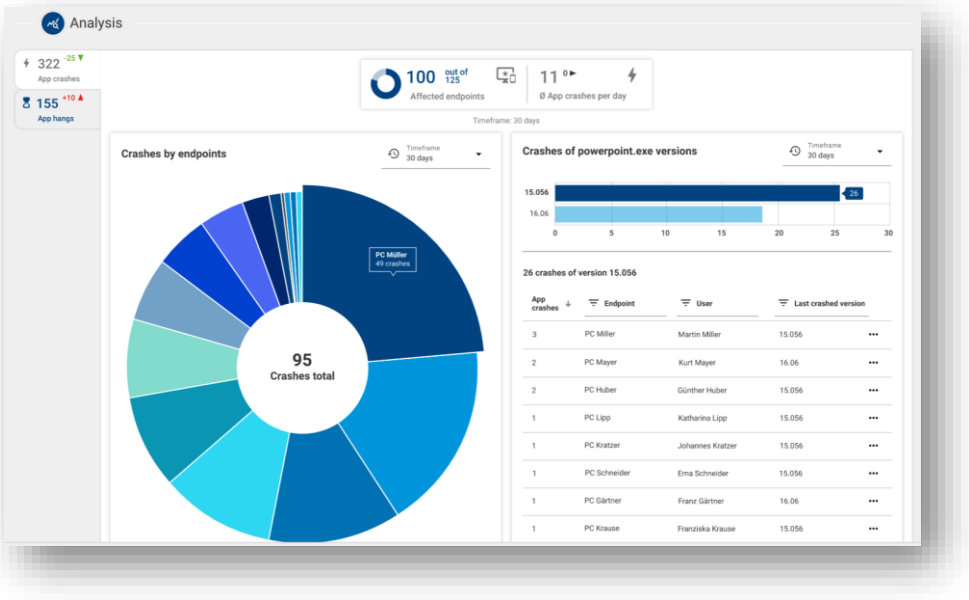


Abbildung 43 - Detaillierte Anzeige von Applikationsabstürzen

Die IT-Admins können diese Frustfaktoren mit bEX ausschalten, indem es eine Korrelation aufzeigt, welche Anwendungen in welcher Version verstärkt Programmabstürze oder -abbrüche erzeugen. Diese Applikationen sollten dann schnellstmöglich aktualisiert werden.

2.7.4 Benchmark der Ergebnisse

Mit der Vielzahl an Daten und Auswertungen in Argus Experience kann es der IT-Administration schwerfallen, konkreten Handlungsbedarf zu erkennen. Argus Experience soll aber nicht mehr Arbeit für die IT-Admins erzeugen, sondern soll deren Arbeit effizienter gestalten. Eine Hilfe, die erfassten Daten besser einordnen zu können, ist das Benchmarking der Ergebnisse.

So wird zum Beispiel mit Hilfe der Umgebungsstabilität angezeigt, ob die Umgebung heute im Vergleich zu den letzten Tagen stabiler oder instabiler war und wie gut – oder wie schlecht – sie im Vergleich zu anderen Umgebungen ist, die in baramundi Argus Experience verwaltet werden.

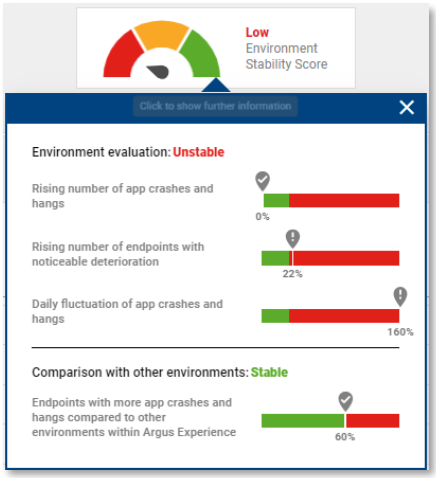


Abbildung 44 - Benchmark der Umgebungsstabilität

Aber nicht nur Vergleiche zu anderen Umgebungen sollen den IT-Admins helfen, sondern auch konkrete Vergleiche einzelner gemessener Daten zu Durchschnittswerten der gesamten Umgebung werden an vielen Stellen in bEX zur Verfügung gestellt.

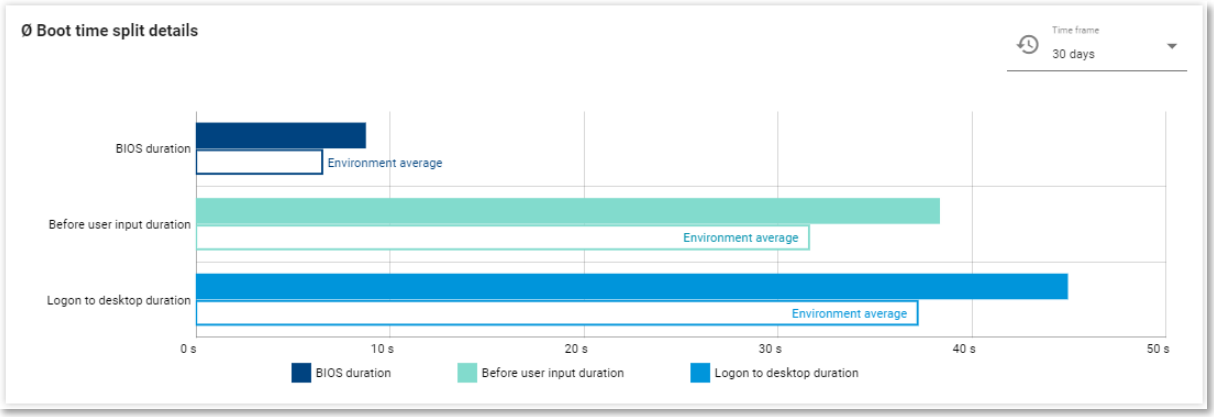


Abbildung 45 - Startzeiten eines Endgerätes im Vergleich zum Umgebungsdurchschnitt

2.7.5 Feedback der End User

Nicht immer liefern die erfassten Stabilitäts- und Performance-Daten der Endgeräte ein ganzheitliches Bild über die IT-Umgebung. Mitarbeiter können oft nicht produktiv arbeiten, weil das Endgerät schlecht performt oder die Software instabil läuft. Manchmal erstellen die Mitarbeiter dann ein Ticket, aber sehr oft lernen sie auch mit den Unzulänglichkeiten und Einschränkungen zu leben, und das ursächliche Problem auf ihrem – und vielleicht auch weiteren Endgeräten – wird nicht analysiert und behoben.
Folglich ist es entscheidend, dass nicht nur Daten der Endgeräte analysiert werden, sondern auch Feedback der End User erfasst und in Korrelation zu den gesammelten Daten gestellt wird, damit IT-Admins effizient und die End User produktiv arbeiten können. Mit Argus Experience ist es möglich[4], das Feedback der End User regelmäßig zu erfassen und auszuwerten.

[4] Diese Funktionalität wird vsl. Ende 2023 in baramundi Argus Experience zur Verfügung stehen.

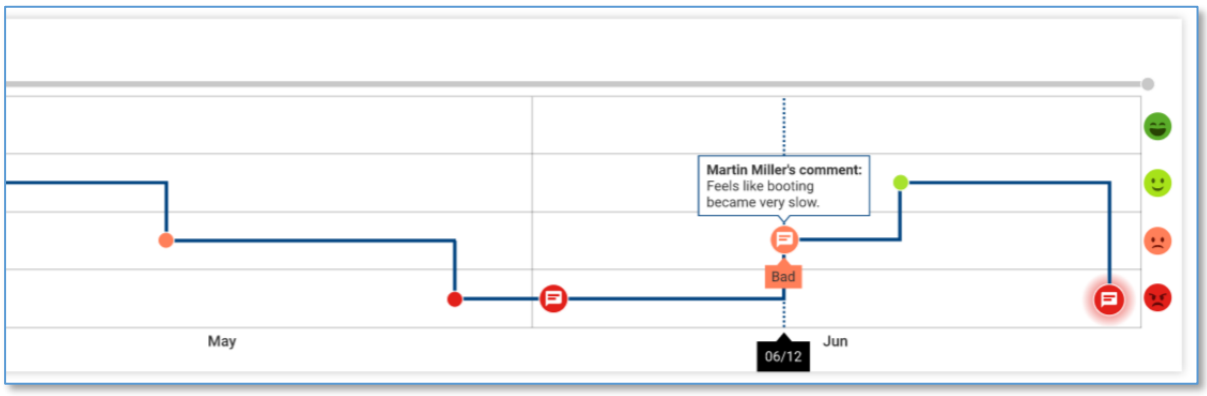


Abbildung 46 – Mitarbeiter-Feedback zu seinem Endgerät

Dieses Feedback kann der Mitarbeiter sehr unkompliziert über den Tray Notifier geben und die IT-Administration kann vorab definieren, ob und mit welcher Regelmäßigkeit die Rückmeldungen der End User eingeholt werden sollen.

Damit ergibt sich für den IT-Admin ein umfassendes Bild über die IT-Umgebung und trägt dazu bei, dass die Mitarbeiter angenehm und sicher arbeiten können.

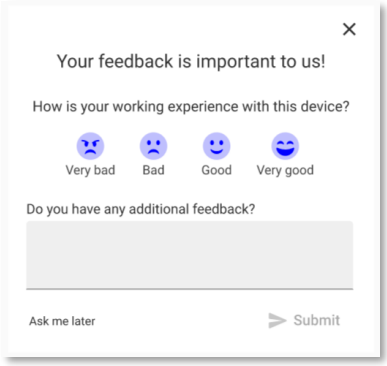


Abbildung 47 – Tray Notifier für End-User-Feedback

2.8 Sonstiges

2.8.1 Identifizierung von Endpoints anhand UUID (Preview)

Der Universal Unique Identifier – kurz UUID – wird bei modernen Computern in der Firmware (UEFI) hinterlegt und ermöglicht die eindeutige Identifizierung des Systems. Im Kontext des Endpoint Managements ist es unerlässlich, die Ziele für die durchzuführenden Managementaktionen zweifelsfrei zu identifizieren, um nicht, zum Beispiel, versehentlich den falschen Endpoint zurückzusetzen.
Ist ein baramundi Management Agent installiert, verwendet die bMS ein clientseitiges Zertifikat, um die Identität zu bestätigen – was aber, wenn ein System neu installiert werden soll und noch kein Agent installiert sein kann? In diesem Fall wird bisher beim Netzwerkboot die MAC-Adresse der Netzwerkkarte verwendet. Mit zunehmend schlankerer Hardware sind häufig keine Netzwerkanschlüsse mehr an den Geräten zu finden – so müssen externe Netzwerkadapter in Form von Dongles oder Docking Stations verwendet werden, welche eine eindeutige Identifizierung anhand der MAC-Adresse erschweren.

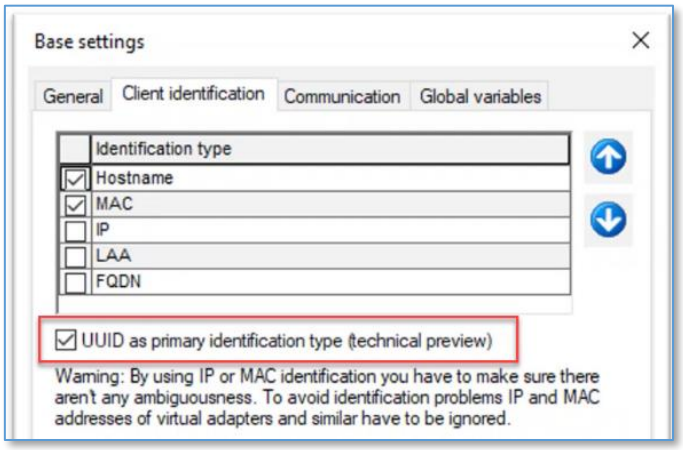


Abbildung 48 - Aktivierung der UUID-Unterstützung

Um weiterhin eine zuverlässige Identifizierung zu gewährleisten, unterstützt die bMS nun auch das Identifizierungsmerkmal UUID – zunächst allerdings nur eingeschränkt, bspw. in Szenarien, in denen die UUID (in der bMS) bekannt ist. So können z. B. Endpoints, deren UUID per Agent übertragen wurde, mit OS-Install neu installiert werden. Neue Endpoints, deren UUID noch nicht an die bMS übertragen wurde, können im Preview nur installiert werden, wenn die UUID zuvor manuell am Endpoint-Objekt in der bMC hinterlegt wurde – eine automatische Erfassung während des Bootvorgangs ist noch nicht möglich.

Hinweis: Werden die für den Netzwerkboot benötigten DHCP-Optionen per Konfiguration am DHCP-Server gesetzt, ist in der Preview zusätzlich noch eine MAC-Adresse zur Identifizierung nötig.

2.9 Produktverbesserungen im Detail

2.9.1 Umgesetzte Abkündigungen / Entfernte Eigenschaften

- Die Reports „Comparex Miss Marple“ werden nicht mehr unterstützt und wurden entfernt.
- Der baraDIP Übertragungsweg HTTP wurde entfernt. Es wird jetzt ausschließlich HTTPS unterstützt.
- Die Dokumentationsdatei für das Datenbankschema steht nicht mehr zur Verfügung. Zum Zugriff auf baramundi Daten wird bConnect empfohlen.
- Unter `Applikation – Installation – Paralleler Installationsmechanismus`, sowie `Applikation – Deinstallation – Paralleler Deinstallationsmechanismus` wird seit der 2023 R2 nur noch das `baramundi Deploy Script` (bDS) unterstützt. Damit fällt das veraltete `baramundi Deploy Package` und `Rational Visual Test 6.5` weg. Es ist zwar noch in der bMC auswählbar, wird jedoch nicht mehr supportet.
- Das Modul `baramundi Virtual`, inklusive des Jobschritts `Virtuelle Maschine verwalten` wird zur Version 2023 R2 eingestellt und steht dann nicht mehr zur Verfügung. Es ist zwar noch in der bMC auswählbar, wird jedoch nicht mehr supportet.

2.9.2 Allgemein

- Die Signierung unserer Setups/Dateien zeigt jetzt als Hersteller baramundi software GmbH, statt baramundi software AG an.
- Bei Neukunden wird das veraltete Patchmanagement Patches (Classic) nicht mehr in der bMC angezeigt. Bestandskunden wird empfohlen auf den Jobschritt `Microsoft Updates verwalten` umzustellen. Die Bereitstellung der Patchdaten `bpmdata3_reduced_signed.zip/bpmdata3_ signed.zip` wird zum April 2024 eingestellt.
- Wird eine Eval-Lizenz (z.B. in der Testumgebung) verwendet, so ist das veraltete Patchmanagement Patches (Classic) nicht mehr in der bMC ersichtlich.
- Die baramundi Lizenzierung erlaubt jetzt auch die Angabe eines Aktivierungsdatums, das Datum ist einsehbar unter `bmc – Konfiguration – Lizenzkonfiguration – Lizenzen`.

2.9.3 Windows Agent (bMA)

- Wird vom bMA ein Neustart des Geräts angestoßen, so erhält der Benutzer jetzt einen weiteren Hinweis in Form einer Dialogbox, womit er den Neustart um einige Sekunden verzögern kann.

- Unter `bMC – Konfiguration – Server – Management Agent` kann über die Option `Erlaube setCustomVar über BMACMD` eingestellt werden, ob das Setzen von Variablen über BMACMD.exe vom Client aus erlaubt ist. Nach dem Update ist die Option eingeschalten. Bei neuen Datenbanken per Default abgeschaltet.

- Das baramundi TrayNotifier-Fenster kann nun nicht mehr versehentlich mittels Alt+F4 oder ESC-Taste geschlossen werden.

- Bei der Ausführung einer Dateikopier-Operation eines bD-Skripts werden jetzt falsche Pfadangaben durch Whitespaces am Anfang oder Ende des Pfades automatisch korrigiert. Damit arbeitet jetzt auch die Kopieraktion bei der Treiberinstallation für Surface Pro 9 Geräte korrekt.

- Bugfix: Der am Job eingestellte Timeout wird zurückgesetzt, wenn die Situation „*es ist bereits ein Job aktiv*“ auftritt. Ggf. wird dann der Job am Client nie automatisch abgebrochen.

- Bugfix: Die Hardware-Inventur läuft bei speziellen Windows 11 Clients auf den Fehler „clinvent.exe hat kein Ergebnis zurückgeliefert“. Damit ist das bDX Update „Upgrade_hwinfo.dll_to_v7.47.bdx“ nicht mehr notwendig

- Bugfix: Werden in Jobs Variablen über bMACMD.exe gesetzt, so kann es auf dem bServer zu Performanceeinbußen kommen, wenn eine große Anzahl an Variablen gesetzt und der Job auf vielen Clients gleichzeitig ausgeführt wird.

- Bugfix: Die Softwareinventur benötigt bei einigen Systemen sehr viel Speicher und stürzt u.U. mit Fehlercode 309 ab.

- Bugfix: Eine (Offline) Softwareinventur läuft auf einen SQL Fehler, wenn sehr lange Dateipfade erfasst werden.

- Bugfix: Wird eine Applikation mit der Option `Applikation startet Rechner neu` verteilt, so wartet der bMA nach dem Ende der Installation nur 120 Sekunden auf den Reboot und löst dann selbst den Reboot aus. (Jetzt wird bis zum Jobtimeout auf den Reboot gewartet).

- Bugfix: In seltenen Fällen kann der Agent die Hash-Validierung von MSW-Dateien nicht durchführen und der Job bricht mit Fehler „Die Hashes zur Dateivalidierung konnten nicht vom Server abgefragt werden“ ab. Die Fehlerhäufigkeit wurde deutlich reduziert.

2.9.4 Management Center (bMC)

- Der `Name` beim `Industriellen Steuergerät` muss nicht mehr eindeutig sein. Es können jetzt beliebig viele Geräte mit gleichem Namen angelegt werden.
- Die Einstellung für den `Sicherheitskontext` unter `Job - Schritt - Serverseite Aktion` wurde umbenannt in `bServer Kontext (LocalSystem oder Dienstbenutzer)` damit klar ersichtlich ist, welcher Benutzer zur Ausführung des baramundi Deploy Skripts verwendet wird.
- Unter `bMC - Umgebung - Client - Übersicht` wird die Version des Betriebssystems auch bei Clients mit Windows 11 IoT Enterprise korrekt erkannt/dargestellt.
- Beim Kopieren einer `Universellen Dynamischen Gruppe` wird der Name und der Anzeigename angepasst, wenn beide davor gleich waren.
- Wird versucht einen Client in den Internet-Modus umzuschalten obwohl kein Gateway konfiguriert ist, so erscheint eine Hinweismeldung.
- `Dynamische Gruppen (Universell)` können jetzt innerhalb anderer `Dynamischen Gruppen (Universell)` verwendet werden.
- Bugfix: Ist unter `bMC - Inventur - Netzwerk Scan` an einem SNMP Profil ein Passwort hinterlegt, so wird dieses beim erneuten Öffnen der Konfiguration überschrieben.
- Bugfix: Am automatisch angelegten Energie-Asset für Monitore werden die Energiedaten auch für den Standby-Betrieb angezeigt, obwohl diese nicht erfasst werden können.
- Bugfix: Wird eine `Dynamische Gruppe (Universell)` mit der Eigenschaft `Primary IP ist leer` oder `ist nicht leer` erstellt, so erscheint ein weiteres unnützes Eingabefeld.

- Bugfix: Wird eine `Dynamische Gruppe (Windows)` so verändert, dass diese ein ungültiges `SQL-Statement` enthält, ist zwar kein speichern möglich, jedoch verschwindet nach Verlassen des Dialogs über `Abbrechen` die Dynamische Gruppe aus der bMC und erscheint erst nach einem Modulneustart wieder.

- Bugfix: Die Option `Job – Erweitert – Bei Jobende Screen Saver aktivieren` hat keine Auswirkung. Diese Option wurde entfernt. Falls diese im Job gesetzt war wird automatisch auf `keine zusätzliche Aktion` umgestellt.

- Bugfix: Unter `bMC – Inventur – Softwareerkennungsregeln` ist das Löschen von Regeln nicht möglich, wenn die Spalte `Typ` ausgeblendet wurde.

- Bugfix: In Multi-Domänenumgebungen ist die Anmeldung an der bMC teilweise nicht möglich, wenn die Zugangsberechtigung über eine Gruppenmitgliedschaft konfiguriert ist.

- Bugfix: Wird ein existierender Job über bDX-Import erneut eingelesen, so werden bereits durchgeführte Jobschritte gelöscht und können dadurch nicht mehr nachvollzogen werden.

- Bugfix: Einige HTML Ansichten verdecken die Anzeige einer bMC-Notification.

- Bugfix: `Persönliche Benachrichtigungen`, welche im Intervall ausgegeben werden sollen, erscheinen nicht genau im angegebenen Intervall.

- Bugfix: Wird der Dialog `bMC – Konfiguration - Server - Einstellungen - PXE-Unterstützung` geöffnet und mit OK bestätigt, so wird zum Neustart des bServers aufgefordert, auch wenn keine Änderungen vorgenommen wurden.

2.9.5 OS-Install

- Die Option `Domäne erst nach der Betriebssysteminstallation beitreten` unter `bMC – Betriebssystem – Hardwareprofile – Hardwareprofil` wurde entfernt.

- Im `Boot Media Wizard` ist jetzt x64 UEFI der Default.

- Bugfix: Beim Hinzufügen eines Treibers über die veraltete Methode `bMC – Betriebssysteme – Treiber – Neu – Windows-Treiber` erscheint u.U. ein Datenbankfehler.

- Bugfix: ist unter `bMC – Konfiguration – Boot-Umgebungen` an einer Boot-Umgebung die Option `Sichtbar im Bootmenü` nicht gesetzt, so kann diese auch im Job oder durch Einstellung am Client nicht korrekt verwendet werden.

2.9.6 Microsoft Autopilot

- Unter `bMC – Konfiguration – Automatische Registrierung – Microsoft Autopilot` kann im Feld `Azure AD Gruppen-ID` eine Azure-AD-Gruppe hinterlegt werden. Es werden dann nur Geräte dieser Gruppe in die bMS synchronisiert.
- Beim Synchronisieren wird jetzt versucht neue Autopilot-Geräte mit bereits bestehenden Geräten Anhand der Mac-Adresse und dem Hostname zu matchen. Damit werden auch bestehende Geräte als Autopilot-Geräte markiert.
- Bugfix: Falls beim Synchronisieren von Autopilot-Geräten ein Fehler auftritt, bricht der gesamte Vorgang ab.
- Bugfix: Die Seriennummer von Autopilot-Geräten bei jedem Autopilot-Sync durch die Hardware-ID überschrieben.

2.9.7 Mobile Devices

- Das Enrollment von Android Enterprise Geräten ab Android 9 ist mittels Android Zero Touch ist möglich
- Im Template für das Management von Dedicated Devices auf Android-Geräten kann nun die Start-Activity einer App angegeben werden, die anstelle der Default-Activity gestartet wird.
- In einer Universellen Dynamischen Gruppe kann die Bedingung `Apple Silicon ja/nein` verwendet werden.
- Der Android Enterprise Agent versteht jetzt den Befehl `ImproveLocationAccuracy` um die Genauigkeit der Standortermittlung am Gerät konfigurieren zu können. Ausgeführt werden kann dieser durch einen `Befehl ausführen – Android Enterprise` Schritt. Weiterhin gibt es einen Fallback für den Befehl `GetLocation`, so dass zumindest ein grober Standort zurückgegeben wird.
- Am Android-Enterprise Gerät wird unter Geräteinventur jetzt auch `Ultra-wideband (UWB)` mit angezeigt.

- Bugfix: Die Rechtevererbung für den Knoten `bMC – Konfiguration – Automatische Registrierung – Apple Automated Device Enrollment` arbeitet nicht korrekt.
- Bugfix: Die Suche nach IOS Geräten unterstützt keine Telefonnummer, ICCID und IMEI.
- Bugfix: Beim Installieren eines Enterprise Wifi auf Android Enterprise Geräten erscheint u.U. die Fehlermeldung "The enterprise network is missing either the root CA or domain name". Um das Profil korrekt installieren zu können, ist jetzt unter `bMC – Erweiterungen – Profile für mobile Geräte` die Angabe einer Domäne am Wi-Fi Profilbaustein möglich.
- Bugfix: Liefert ein iOS-Gerät nicht valide XML Daten, z.B. den Namen eines CurrentCarrierNetwork in der Hardwareinventur, so können auf diesem System keine Jobs mehr ausgeführt werden.
- Bugfix: Die, in der bMC angezeigte Enrollment URL für Android Enterprise Geräte, führt auf dem Endgerät zu einem Fehler. Der QR-Code arbeitete aber korrekt.
- Bugfix: Um MDM-Jobs bearbeitet zu können werden Rechte auf `bmc – Umgebung` benötigt.
- Bugfix: Wird versehentlich ein Benutzer von einem Android Enterprise Gerät gelöscht, so kann dieser nicht wieder gesetzt werden. (Jetzt wird ein AD-Sync den Benutzer wiederherstellen).

2.9.8 bServer

- Jobs mit Schritten für `Serverseitige Aktionen` (SSA) benötigen jetzt im Sicherheitskontext LocalSystem keine interaktive Anmeldung mehr und werden daher auch in gehärteten Umgebungen ausgeführt.
- Verbesserte Datenbankabfragen beim Neustarten von Jobtargets, welche zu deutlich weniger SQL-Deadlocks führen.
- Bugfix: Bei Jobs, welche per Intervall eingeplant sind, wird der Fehlerzähler für `Wiederholung im Fehlerfall` auch nach einem erfolgreichen Durchlauf und dem Neuplanen des Jobs nicht zurückgesetzt.

- Bugfix: Unter `bMC – Persönliche Einstellungen – Benachrichtigungen` hinterlegte Benachrichtigungen führen u.U. nach dem Löschen des Benutzers dazu, dass sich auch andere Benutzer nicht mehr an der bMC anmelden können.

2.9.9 AD-Sync

- Am AD-Benutzer (`bMC – Umgebung – Benutzer und Gruppen)` sind jetzt zusätzlich die Felder `Vorname`, `Nachname` und `Vorgesetzter` verfügbar.
- Bugfix: Sind im AD bestimmte Replikationsojekte vorhanden, so läuft ein `Benutzersynchronisationsjob` u.U. auf den Fehler „Object reference not set to an instance of an object“.
- Bugfix: Ein `Benutzersynchronisationsjob` läuft u.U. dauerhaft auf Fehler, wenn im AD eine Benutzergruppe verschoben wurde.

2.9.10 PXE-Relay

- Bugfix: Client bleibt beim Bootvorgang über ein PXE-Relay in der PXE-Phase hängen, wenn Boot ohne DHCP Optionen verwendet wird.
- Bugfix: Ist die Latenz vom PXE-Relay zur Datenbank groß, so kann es beim Öffnen der bMC auf dem PXE-Relay (um das PXE-Relay zu konfigurieren) zu einem Timeout kommen. Die maximale Wartezeit hierfür wurde deutlich erhöht.

2.9.11 bConnect

- `networkEndpoints` sind verfügbar.
- `sshConfiguration` und `snmpProperties` können gelesen werden.
- Abfrage des `PatchLevel` am AppleEndpoint ist verfügbar.

2.9.12 Netzwerkgeräte

- Eine Miniinventur für ausgewählte Linux-Distributionen ist möglich. Die ermittelten Daten können in Universellen Gruppen verwendet werden und stehen auch über bConnect bereit.
- Die Angabe eines `Registrierter Benutzer` an einem `Netzwerkgerät` wird jetzt unterstützt.

- Im `Job für OT oder Netzwerkgerät` sind jetzt Schritte `Skriptausführung über SSH` möglich.
- Unter `bMC – Inventur – Netzwerk-Scan – Profil` gibt es eine neue Einstellung `Vorhandene Geräte außerhalb der Gruppe ignorieren`.
- Unter `bMC – Inventur – Netzwerk Scan – Profile` kann jetzt schnell über den Button `Netzwerk-Scan Job anlegen` ein Job generiert werden.
- Unter `bMC – Umgebung` kann am Netzwerkgerät, sowie am Industriellen Steuergerät eine `Persönliche Benachrichtigung` konfiguriert werden.
- Bugfix: Wird ein Kommentar am Netzwerkgerät gesetzt, so wird dieser u.U. durch einen weiteren SNMP-Scan zurückgesetzt.
- Bugfix: Unter `bMC – Inventur – Netzwerk Scan – Erkennungsregeln` können bestimmte valide OID nicht konfiguriert werden, da diese als invalid abgewiesen werden.

2.9.13 macOS

- Bugfix: Einige Geräte werden falsch erkannt, z.B. wird ein MacBook Air M2 als iMac 27" (Late 2013) erkannt.
- Bugfix: Die Installation von lokalen macOS PKGs größer 2 GB schlägt mit der Meldung "No manifest data recieved" fehl.

2.9.14 baraDIP

- Der baraDIP Dienst für bBT-Transfer und DipSync wurde tiefgreifend überarbeitet. Hinweis: eine bMS-Version 2023 R2 oder höher ist nicht mit älteren baraDIP kompatibel. Beim Update ist daher ein zeitnaher Austausch der baraDIP Dienste auf allen DIP-Servern zwingend.
- Unter `bMC – Konfiguration – DIP – DIP-Verwaltung` kann jetzt komfortabel für einzelne DIP-Server die Vertrauensstellung durch `TLS zurücksetzen` entfernt werden und durch `TLS konfigurieren` wieder hergestellt werden.

3 Release 2023 R1

3.1 Windows Schwachstellenkatalog 2.0

Um auch weiterhin zuverlässig Schwachstellen an den Endpoints erkennen zu können, werden in Zukunft einige Änderungen im baramundi Vulnerability Scanner durchgeführt. Der Startschuss erfolgte zum Jahresanfang durch umfangreiche Änderungen an den Schwachstellenkatalogen.

Zu Beginn der Umstellung wurde zunächst das Scanprofil „Community“ entfernt. Dieses Profil wurde bereits seit Einführung des Vulnerability Scanners ausgeliefert und war anfangs der einzige Katalog. Seither wurde dieser Katalog von der Community nur noch sporadisch mit Regeln versorgt und so haben wir im Jahr 2016 einen neuen Katalog hinzugefügt: das Profil „Professional“. Aus Kompatibilitätsgründen haben wir das „Community“-Profil beibehalten, obwohl hier kaum neue Regeln hinzukamen.

Der Katalog, auf dem das „Professional“-Profil beruht, ist in den letzten Jahren sehr stark gewachsen. Die Zeit zum Prüfen aller Regeln erhöhte sich teils drastisch und eine neue Lösung war nötig: Das neue Profil „Professional 2.0“! Dieses Profil basiert auf einem neuen Katalog mit optimiertem Regelwerk, welches auf eine geänderte Mechanik und auch Logik setzt, um Schwachstellen zu erkennen. Im Vordergrund steht dabei, vorhandene Softwareinstallationen und nicht mehr nur die reine Existenz einzelner Dateien, Bibliotheken oder Komponenten zu erkennen.

Umfangreiche Informationen finden Sie in unserem Blogbeitrag:
https://www.baramundi.com/de-de/blog/artikel/neuer-schwachstellenkatalog-2-0/

3.2 bConnect 2.0

In der heutigen IT werden verbundene Systeme zunehmend relevanter. Die Anfragen nach einer konformen und mitwachsenden Schnittstelle mehren sich. Unsere bisherige bConnect 1.x Schnittstelle lieferte vielen Umgebungen eine Möglichkeit, Projekte umzusetzen. Die Eigenentwicklung zog jedoch einen Pflegeaufwand in Controllern und der manuellen Pflege der Dokumentation mit sich.
Mit der Weiterentwicklung unserer Schnittstelle bConnect 2.0 folgen wir nun gängigen API-Konformitäten, indem wir auf OpenAPI[5] basieren.

3.2.1 Umgang mit Daten

Durch die Umstellung der darunterliegenden Technologie hat sich die Geschwindigkeit der einzelnen Aufrufe merklich beschleunigt. Dies wird vor allem bei Programmteilen mit vielen Aufrufen spürbar.
Die dabei abgerufene Datenmenge wurde auf das Wesentliche reduziert, um nicht alle Objekte laden zu müssen. Dies ist durch Paging-Ergebnisse besser zu handhaben und wirkt früheren Timeouts (30 Sek.) bei größeren Abfragen wie bspw. der Abfrage nach <Alle Endpoints> entgegen.

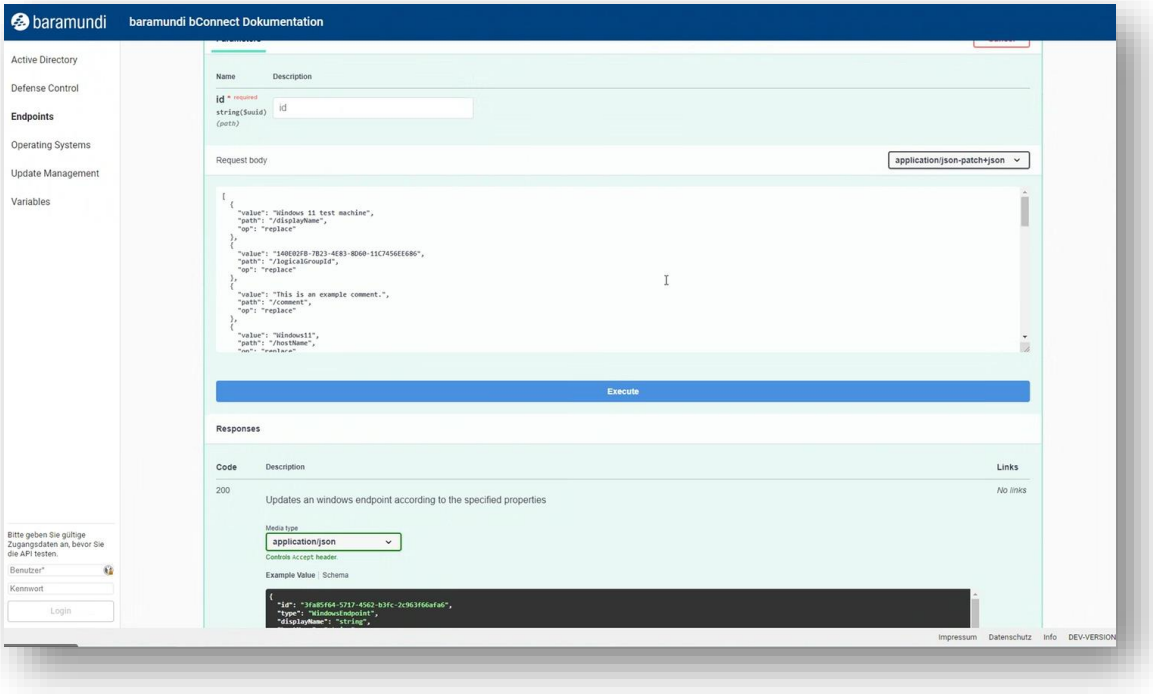


Abbildung 49 - bConnect 2.0 Funktionsdetails

[5] https://www.openapis.org/

3.2.2 Struktur

Der Aufbau der einzelnen Controller ist im Web-Interface der API direkt einsehbar und per Knopfdruck bereits ausführbar.
Dies bedeutet, dass neben einer „Live“-Übersicht der möglichen Funktionen (ohne separates Dokument) und Menüführung durch den Navigationsbaum auf der linken Seite in jeder einzelnen Funktion direkt mit Parametern und Beispiel-Calls gearbeitet werden kann.

Das führt nicht nur zu einer besseren Übersicht über die Gesamtheit der API, sondern hilft auch bei der Vermeidung von Fehlaufrufen oder falschen Parametern.

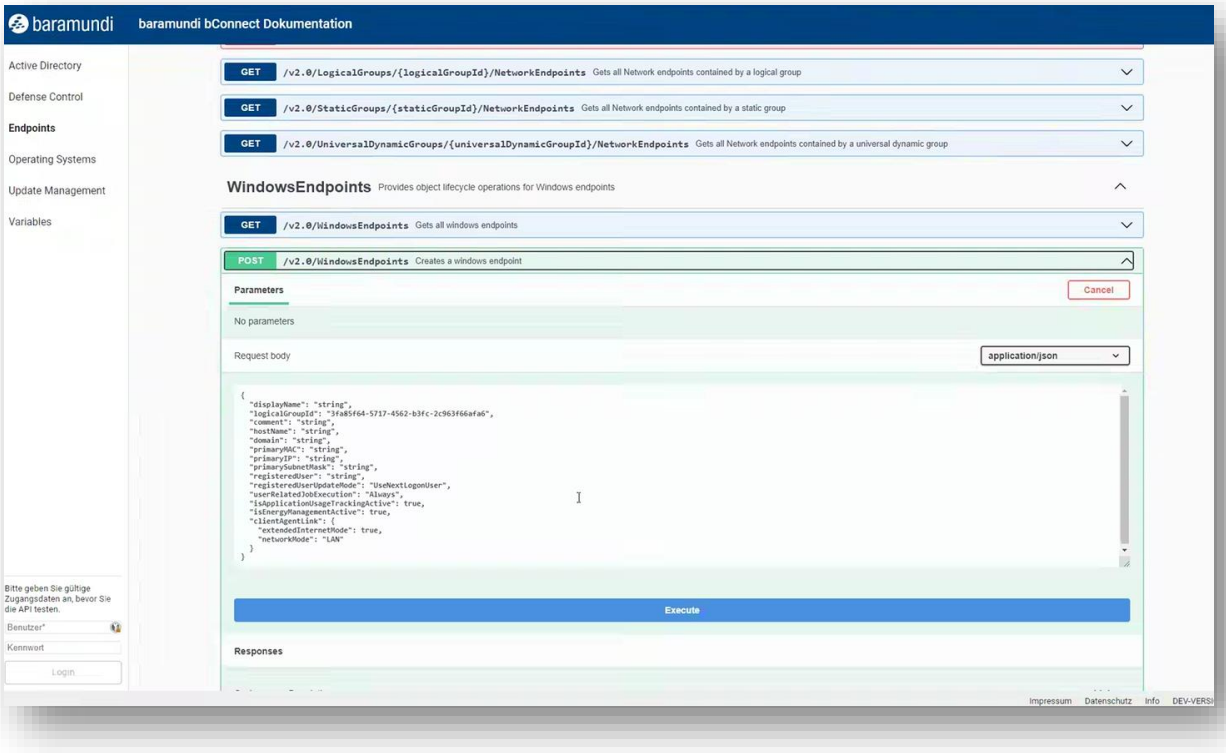


Abbildung 50 - bConnect 2.0 Controller - Funktionsliste

3.2.3 Weiterentwicklung

Der initiale Funktionsumfang von bConnect 2.0 enthält die folgenden Controller:

Controller	Beschreibung
Active Directory	vom Active Directory bezogene Objekte wie Benutzer, Gruppen oder Organisationseinheiten
Endpoints	die primären Objekte der baramundi Umgebung wie bspw. Windows-, Android-, iOS-, Mac-, Industrial- sowie Network-Endpunkte
Operating Systems	verwaltet die OS-Installationsinformation und -konfiguration für Windows-Endpunkte
Update Management	verwaltet die Update Management-Information und -Konfiguration für Windows-Endpunkte
Variables	Variablen sind ein wesentlicher Bestandteil der baramundi Management Suite. Der Controller ermöglicht den Zugriff objektübergreifend auf die Variablendefinition sowie die eigentlichen Variablenwerte.

bConnect 1.x steht in der Übergangsphase weiterhin zur Verfügung, um die Funktionen beider Schnittstellen kombinieren zu können. Die oben genannten Controller wurden bereits in bConnect 2.0 implementiert. Darüber hinaus bietet bConnect 2.0 nun folgende zusätzliche Funktionen an:

- Endpunkte und/oder Clients deaktivieren
- AD-Benutzer und -Gruppen sind nun auslesbar
- Variablenzugriff auf AD-Objekte

Die komplette Umstellung der API auf OpenAPI ermöglicht nun eine konsistente und einfachere Umsetzung künftiger Funktionen und Erweiterungen für unsere Schnittstelle.

3.3 baramundi Ticketing System [Preview]

Das neue Release des baramundi Ticketing Systems ist für Sommer 2023 geplant. Die folgende Übersicht beschreibt die Highlights der geplanten neuen Funktionen und Änderungen.

Technologie und Design des Benutzerclients werden vollständig überarbeitet. Dadurch ergeben sich für das gesamte System neue Möglichkeiten und neue verbesserte Benutzeroberflächen. Diese Möglichkeiten werden auch für zukünftige Releases genutzt, um die Benutzererfahrung stetig zu verbessern.

Das Thema Barrierefreiheit der Anwendung wird in Folge-Releases ebenfalls im Mittelpunkt stehen. Alle gängigen Formulare, Funktionen und Clientbestandteile werden zukünftig vollständig mittels Screenreader auslesbar und per Tastatur bedienbar sein sowie später weitere spezifische Funktionen erhalten.

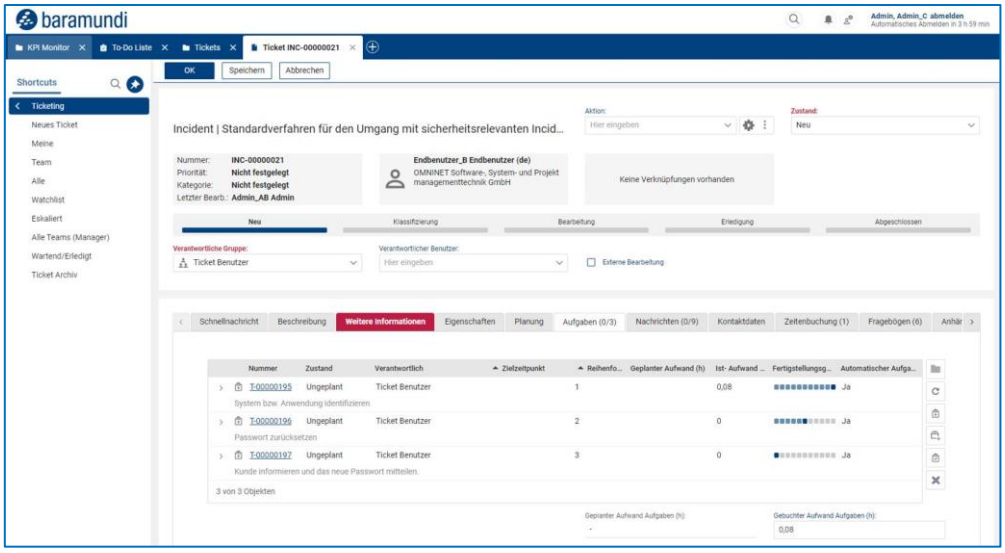


Abbildung 51 – bTS Neues Design

3.3.1 Neues Design

Das Design der gesamten Clientoberfläche (GUI) wird überarbeitet. Alle wesentlichen bestehenden Funktionen werden beibehalten. Die Anordnung und das Aussehen vieler Controls und Felder werden optimiert.

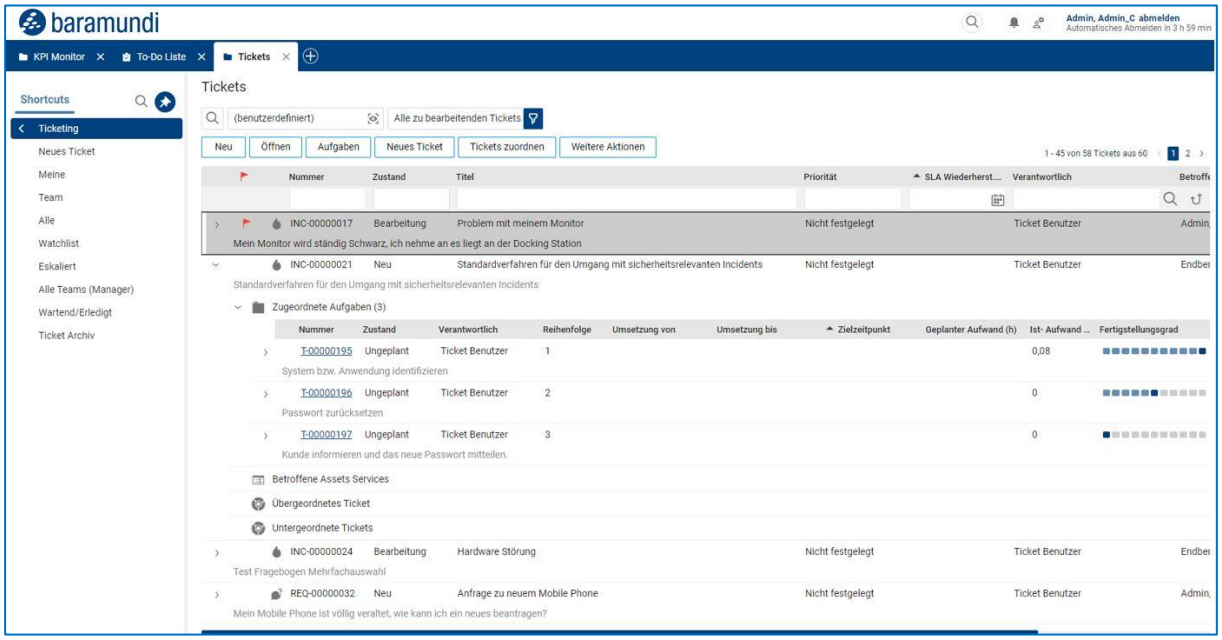


Abbildung 52 - bTS - Ticketliste

3.3.2 Formular Re-Design

Das Design und Aufbau der Formulare für Tickets, Assets, Aufgaben und Wissensdatenbank wird überarbeitet. Hierzu wird die Anordnung der bislang untereinander liegenden Formularsektionen auf nebeneinander dargestellte Tabs umgestellt. Weiterhin werden teilweise die Anordnung und Reihenfolgen der Felder sowie Listen überarbeitet und neu aufgeteilt. Ziel ist es, wichtige Inhalte auf einen Blick zu haben, diese schneller zu erreichen und potenziell langen Listen in Formularen den nötigen vertikalen Platz zu geben.

3.3.3 Verbesserte Performance

Durch Verwendung der neuen Clienttechnologien wird die Performance des gesamten Systems verbessert. An vielen Stellen, vor allem bei vielen Aktionen innerhalb der Formulare (z.B. im Ticketformular), werden dadurch bisherige Wartezeiten um bis zu 90% reduziert.

3.3.4 Neues Session Handling

Beim Login wird jeder Benutzer selbst entscheiden können, ob eine ggf. noch offene Session weiterverwendet werden soll oder diese beendet und eine neue Session mit der Anmeldung genutzt werden soll. Mit dieser Möglichkeit entfällt die Wartezeit bei Anmeldeversuchen bei nicht ordnungsgemäßem Beenden früherer Sessions vollständig.

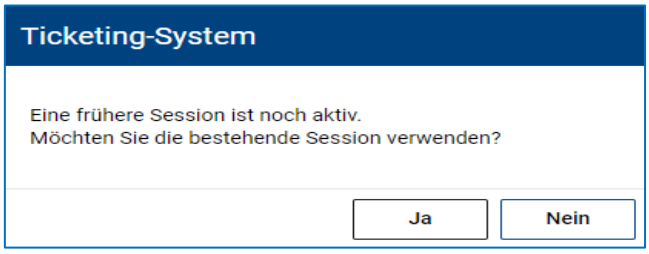


Abbildung 53 - bTS - Sessionübernahme

3.3.5 Mobile Use dank Fully Responsive Design

Der gesamte Client wird fully responsive gestaltet sein. Damit ist eine vollständige Nutzung aller Oberflächen und Formulare auf jeder Bildschirmgröße möglich (einschließlich kleinerer Tablets und Smartphonebildschirmen). Das System erkennt automatisch die Größe des Bildschirms und passt das Oberflächendesign entsprechend an. So können auch problemlos „unterwegs“ alle Funktionen genutzt werden sofern eine Internetverbindung besteht.

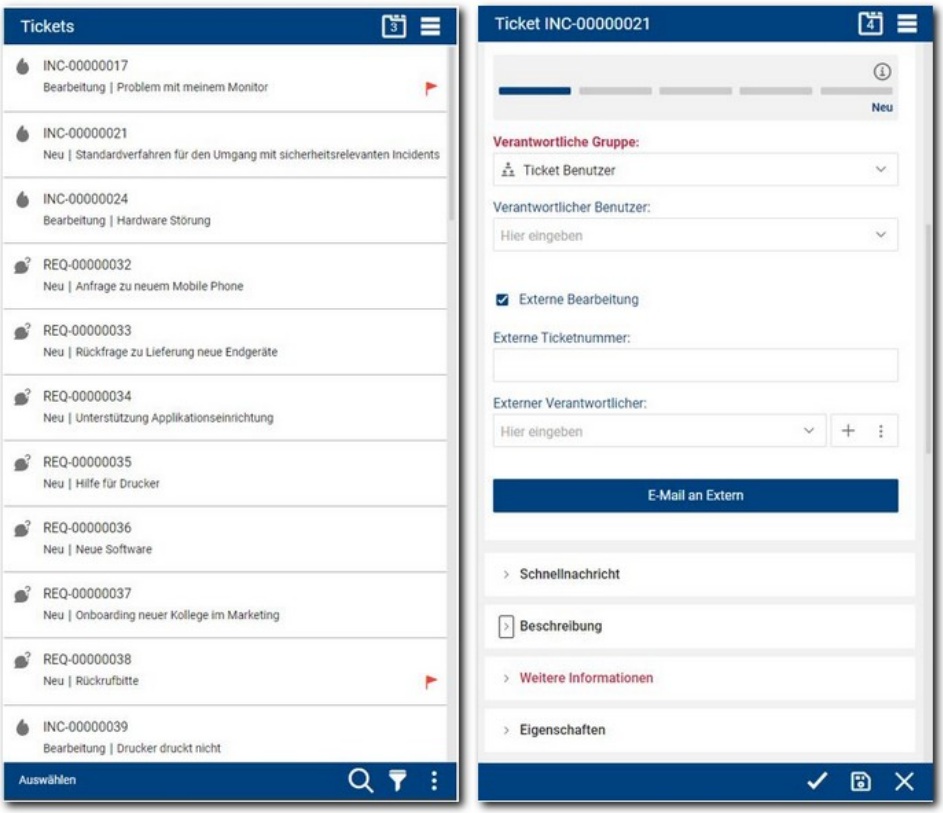


Abbildung 54 - bTS - Mobile Design

3.3.6 Einführung AD Sync für Personen über die bMS Schnittstelle

Dank der neuen bConnect 2.0 Schnittstelle dieser bMS Version können auch die verfügbaren Active Directory-Informationen zu Personen bzw. Benutzern und anderen Variablen direkt aus der bMS im Ticketing System per automatischem und zeitgesteuertem Import aktualisiert werden. Damit müssen Informationen aus dem AD nicht mehr separat in das Ticketing System importiert werden. Zusätzliche Informationen aus anderen Datenquellen können weiterhin auch per CSV importiert und ergänzt werden.

3.4 baramundi Argus Cockpit und Experience [Preview]

Weiterentwicklungen mit diesem Release[6] erleichtern insbesondere die Fehleranalyse bei Supporttickets und verbessern die Übersicht auf relevante IT-Daten.

3.4.1 Mehr UDG in Argus Cockpit

Bisher standen pro Umgebung in baramundi Argus Cockpit zehn UDG zur Verfügung, die mit dem zugehörigen baramundi Management Server synchronisiert werden konnten. Mit der Möglichkeit aus dem letzten Release diese UDG zu „taggen“, hat sich der Anwenderkreis für diese Ansicht deutlich vergrößert. Es ist nicht mehr nur der IT-Admin, der mit den UDG-Kacheln einen schnellen Überblick über wichtige Kennzahlen seiner IT-Umgebung erhält. Auch ein Chief Information Security Officer (CISO) kann beispielsweise spezielle UDG einsehen und deren Ergebnismengen kontrollieren. Um dieser wachsenden Nachfrage gerecht zu werden, können nun mehr UDG pro Umgebung in baramundi Argus Cockpit angefragt werden.

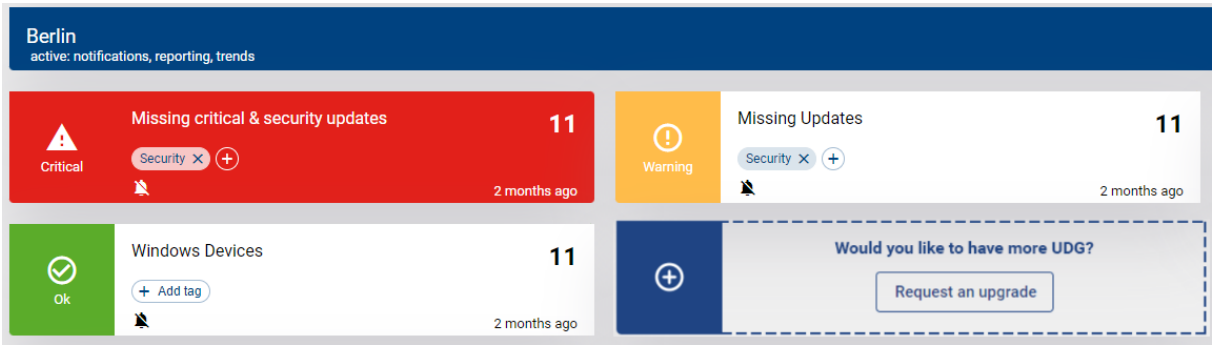


Abbildung 55 - Mehr UDG im Argus Cockpit anfragen

3.4.2 Auffällige Software in Argus Experience analysieren

IT-Admins können in baramundi Argus Experience erkennen, ob es auffällige Endgeräte gibt, auf denen Software häufig abstürzt oder hängen bleibt. Diese Informationen werden um

[6] Marktstart für baramundi Argus Experience ist vsl. Sommer 2023.

weitere Ansichten erweitert, so dass nun auch die auffällige Software analysiert werden kann.
So lässt sich für den IT-Admin schnell herausfinden, ob im gesamten Unternehmen die Software-Abstürze/Hänger eher zu- oder abnehmen und welche Applikationen dabei besonders auffällig sind.

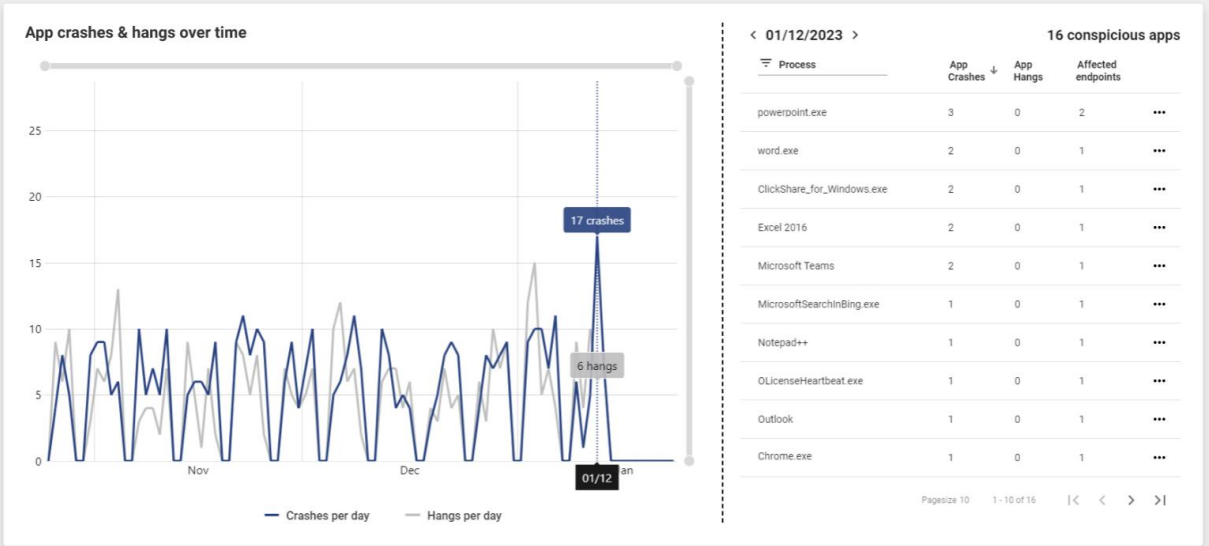


Abbildung 56 - bEX-Preview: Abstürze und Hänger pro Applikation

Entscheidend für die Fehleranalyse und für die anschließende Fehlerbeseitigung ist allerdings, die kritische Softwareversion zu kennen. Detailansichten pro Applikation erlauben es dem IT-Admin zu erkennen, ob es eine bestimmte Softwareversion gibt, die häufiger abstürzt oder hängen bleibt. Diese Information kann er nutzen, um bspw. mit baramundi Managed Software diese auffällige Version – auf einem bestimmten Endgerät oder im gesamten Unternehmen – zu aktualisieren.

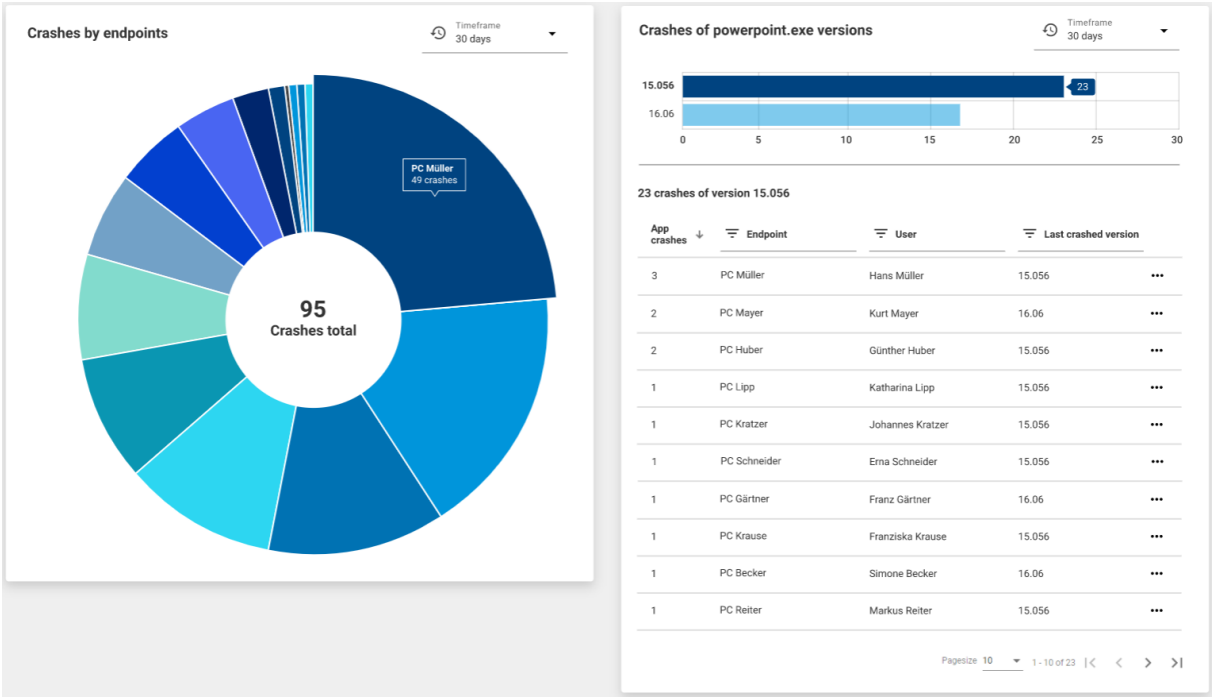


Abbildung 57 - bEX-Preview: Software-Abstürze pro Endgerät und SW-Version

Hat der IT-Admin eine Softwareversion im gesamten Unternehmen ausgerollt, entweder weil er die veraltete Version bereits als „häufig abstürzend“ identifiziert hat oder weil die veraltete Version als unsicher eingestuft wurde, kann er das Ergebnis des Rollouts mit folgender Darstellung einsehen:

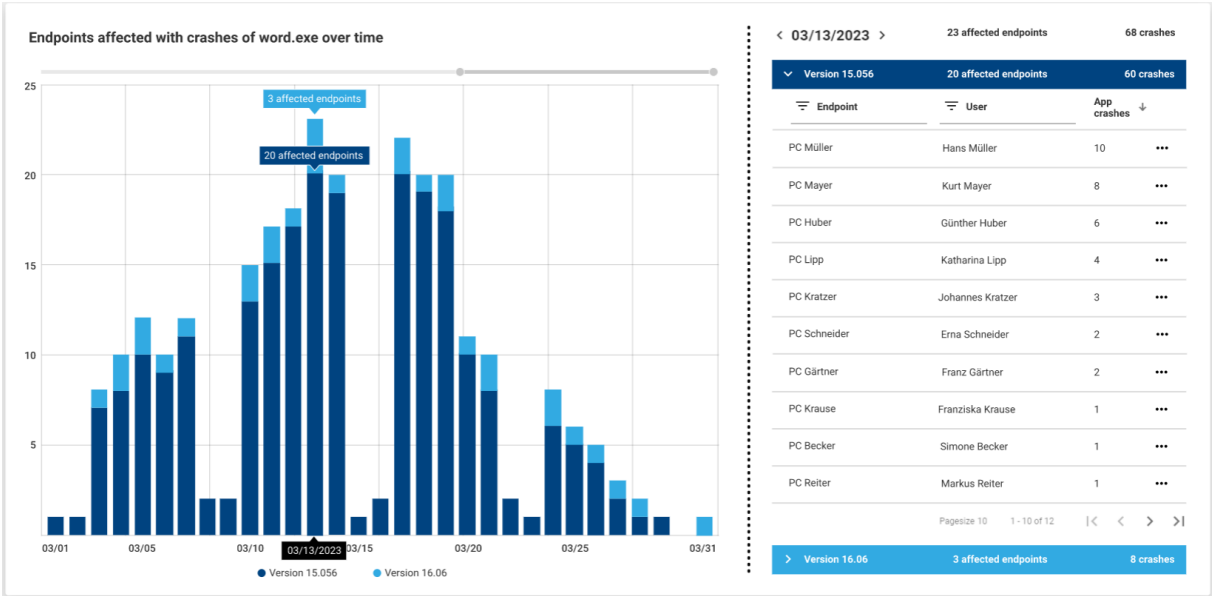


Abbildung 58 - bEX-Preview: Anzahl Endpoints mit auffälligen Software-Versionen

Beispiel: Ab dem 19. März hat der IT-Admin ein Softwareversionsupdate (Version 16.06) im gesamten Unternehmen ausgerollt. Im Diagramm ist erkennbar, dass die Gesamtanzahl der

Abstürze dieser Applikation ab dem 20. März abnimmt und die veraltete Version ab 30. März nicht mehr abstürzt (da durch Version 16.06 ersetzt). In der Folge haben alle End User eine sichere und besser funktionierende SW-Version im Einsatz.

3.4.3 Benchmark der Systemstabilität

Es ist eine Herausforderung für IT-Teams, festzustellen, ob die erfassten Daten der Endgeräte auffällig oder normal sind. Zu entscheiden, ob Handlungsbedarf besteht oder nicht, basiert zumeist auf Erfahrung und „Bauchgefühl“. Ob 20 Abstürze durch 2 Applikationen auf 5 Endgeräten oder 50 Abstürze durch 10 Applikationen auf 20 Endgeräten auffällig sind und Handlungsbedarf anzeigen, ist für IT-Administratoren schwer einzuschätzen.
Eine Erleichterung bei dieser Einschätzung bietet der bEX „Environment Stability Score“.

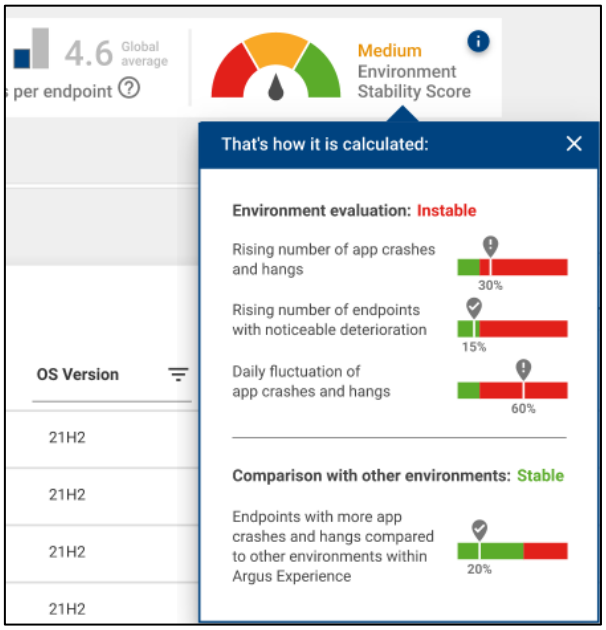


Abbildung 59 - bEX-Preview: Scoring für Einschätzung der Gesamt-Stabilität

Er zeigt an, wie stabil die eigene IT-Umgebung im Vergleich zu anderen IT-Umgebungen ist und es wird erklärt, wie die Anzahl der Software-Abstürze/Hänger in dieses Scoring einfließen.

3.4.4 Fehleranalyse schnell beginnen

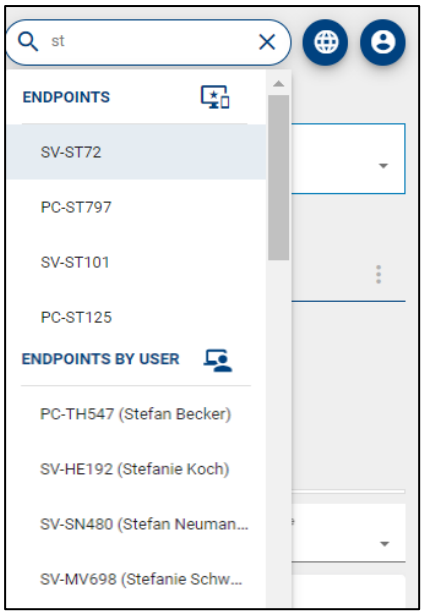


Abbildung 60 - Suche nach IT-Assets

Oft ist die Zeit knapp, um Supporttickets von End Usern schnell und nachhaltig zu lösen. Umso wichtiger ist es,

- das betreffende Endgerät,
- die auffällige Software oder
- den (frustrierten) End User

in bEX schnell zu finden.
Eine neue Suche in baramundi Argus Experience ermöglicht es den IT-Teams, schnell das relevante Suchergebnis aufzurufen und in die Fehleranalyse einzutauchen. Sie finden schnell, wonach sie suchen, und können ihre Zeit effektiver nutzen und ihre Arbeit schneller erledigen.

3.5 Universelle Dynamische Gruppen

3.5.1 Plattformicons

Die universellen dynamischen Gruppen bieten zahlreiche Einsatzszenarien an, um auch über Endpunkttypen hinweg Bedingungen zu erstellen. Um diese Endpunkttypen bei der Auswahl der Bedingungen einfacher zu gestalten, wurden nun die entsprechenden Plattformsymbole des jeweiligen Typs in der Liste hinzugefügt.

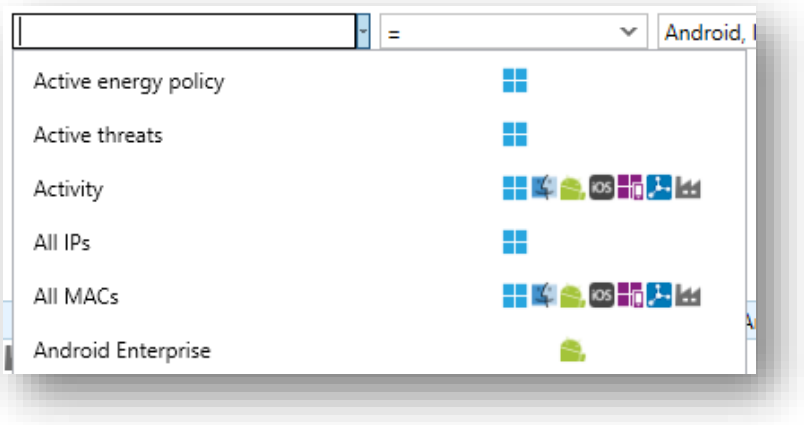
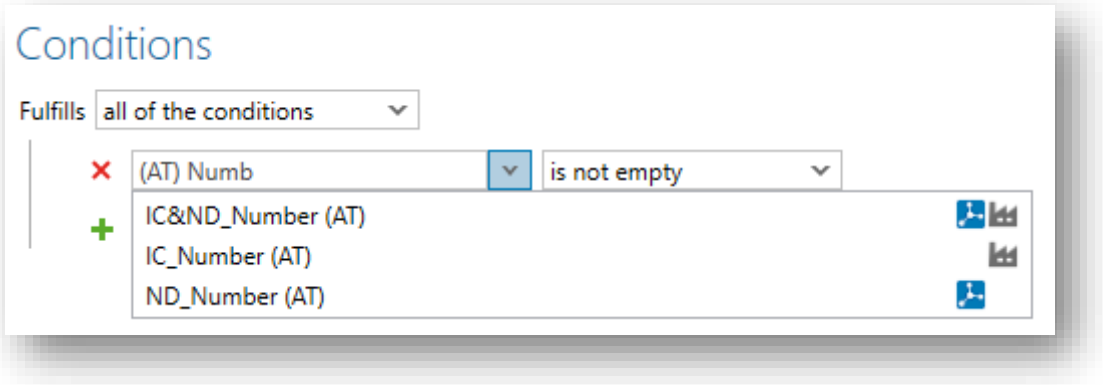


Abbildung 61 - UDG Bedingungen – Icons

3.5.2 Freitextfilter

Es ist nun möglich beim Erstellen/Bearbeiten einer dynamischen Gruppe die möglichen Eigenschaften mit einem Freitextfilter zu filtern. Im Freitextfilter können mehrere Wörter eingegeben werden und jede Eigenschaft, die alle Wörter beinhaltet, wird angezeigt. Bei mehreren Wörtern im Suchtext werden die Wörter unabhängig voneinander gesucht, z.B. "Antivirus status" findet alle Einträge, die sowohl die Wörter "Antivirus" als auch "status" enthalten.



3.6 Produktverbesserungen im Detail

3.6.1 Behebung der bekannten Probleme der bMS 2022 R2

- Die im Forum dokumentierten Probleme der 2022 R2 wurden in der 2023 R1 behoben.
- Die Fehlerbehebung `bMS2022R2-U1` ist in dem Release 2023 R1 enthalten.
- Bugfix: Die bMC Ansicht `Inventory – Software – Windows-Geräte` zeigt unerwartet viele Software an.
- Bugfix: Zum Zuweisen von Jobs wird u. U. auch das `Modify` Recht am Client benötigt.
- Bugfix: Werden Ordner unter `bMC – Umgebung – Dynamische Gruppen` gelöscht, welche `Dynamische Gruppen (Universell)` mit einer konfigurierten automatischen Jobzuweisung beinhalten, so treten im bServer.log stetig wiederkehrende Datenbankfehler auf.
- Bugfix: bD-Skript für Benutzereinstellungen wird u.U. wegen „Zugriff verweigert (code = 5)“ nicht ausgeführt. Hinweis: Der bMA ab 2023 R1 greift jetzt wieder im Kontext des angemeldeten Benutzers auf die User-bDS Datei zu.

3.6.2 Windows Agent (bMA)

- Der Jobschritt `Microsoft Patches verteilen (Classic)` verwendet jetzt zum Ermitteln des Patch-Status auf x64 Systemen die 64 Bit Windows API.
- Der bMA verwendet zur Extrahierung von .cab Dateien nun das systemeigene expand.exe
- Auf der Übersichtsseite von Windows-Endpunkten werden unter `Datenträgerinformationen` nun auch eMMC-Datenträger aufgeführt.
- Bugfix: Die Energieverbrauchsdaten für Clients `im Standby` werden nicht ermittelt und immer als 0 gemeldet, sowie als 0,00 kWh in der bMC am Endgerät angezeigt.
- Bugfix: Die Hardware-Inventur führt bei neueren Systemen zum BlueScreen auf dem Endgerät.
  Hinweis: Leider kann aktuell nicht ausgeschlossen werden, dass auf Systemen mit neuer Hardware weiterhin Bluescreens auftreten.

3.6.3 Management Center (bMC)

- Die Detaildarstellung von `Client – Compliance – Schwachstellen - Erkannt` wurde für den neuen `Vulnerability Scan: Windows (Professional 2.0)` optimiert. Insbesondere sind die `Analysierten Elemente` jetzt sprechender und zeigen nur die relevanten Stellen an.

- Die Konfiguration für Spalten bei Universellen Dynamischen Gruppen (UDG) kann als Default abgespeichert werden.

- Am Windows-Endgerät sind wieder unter `Übersicht – Microsoft Update` die Eigenschaften `Verzögerung von Funktionsupdates` und `Funktionsupdate-Version` sichtbar.

- Der Auswahldialog der Eigenschaften für `Dynamische Gruppe (Universell)` wurde verbessert und durch Symbole der Endpunkttypen erweitert.

- Mit dem Kommandozeilenparameter `/username=n` ist es möglich einen Benutzernamen an den bMC-Anmeldedialog zu übergeben.

- Die Aktion `Logische Gruppierung – Inhalt - Extras – Shutdown/Neustart` benötigt nun keine Einzelbestätigung mehr, wenn mehrere Clients ausgewählt wurden.

- Bugfix: Im Dialog `Software – Managed Software – Einstellungen` werden vorgenommene Änderungen nicht übernommen, wenn diese per Tastaturbedienung durchgeführt wurden.

- Bugfix: Die Anzeige der Crystal Reports ist nicht möglich, wenn im Datenbankmanager zusätzlich ein Port für die Datenbank angegeben ist.

- Bugfix: Zum Zuweisen eines Jobs an einem Endgerät werden neben Jobzuweisungsrechten auch Modify-Rechte benötigt. (Verhalten der 2023 R1 entspricht wieder dem Verhalten der 2022 R1)

- Bugfix: Die Darstellung des Passworteingabefeldes bei `Konfiguration – Domänen` ist teilweise nicht konsistent.

- Bugfix: Unter `Inventur – Netzwerk Scan – Profile` können ungültige Netzwerkprofile mit kleinerer Endadresse als Startadresse im `SNMP IP-Bereich` angegeben werden.

- Bugfix: Unter `Inventur – Asset-Typen` kann bei einem `Asset-Typ` eine ungültige Icon-Datei ausgewählt werden.
- Bugfix: Beim Anlegen eines Assets am Client stürzt u.U. die bMC ab, z.B. wenn sehr viele Assettypen vorhanden sind.
- Bugfix: Die Aktion `Organisieren – Alles nach Excel exportieren` zeigt einen Fehler der Art „*The maximum number of Cell styles was exceeded*.“, insbesondere wenn die zu exportierende Ansicht viele Einträge und viele Spalten beinhaltet.
- Bugfix: Das Öffnen eines Windows Endgerätes in einem Tab dauert u.U. sehr lange, insbesondere wenn es Gruppen mit sehr vielen Clients gibt.
- Bugfix: Auf dem PXE-Relay wird `Konfiguration – Management Center` angezeigt, die dort vorgenommenen Einstellungen werden jedoch nicht gespeichert.
- Bugfix: Die bMC wird unerwartet geschlossen, wenn unter `Jobs – Job – Einstellungen – Übersicht` bei einem `Hardware-Inventarisierung` Schritt auf den Öffnen-Pfeil geklickt wird.
- Bugfix: Einige Elemente wurden im `Theme – Dunkel` mit unleserlichen Farben dargestellt.
- Bugfix: Die Anzeige `Umgebung – Client – Inventur – Software` ist u.U. sehr langsam und das Scrollen in der Softwareliste ist dann nicht möglich.
- Bugfix: In der bMC in der Detailansicht eines Jobtargets wird u.U. die Schrittnummer eines Schritts falsch angezeigt, wenn das Jobtarget gerade ausgeführt wird.

3.6.4 bMUM Windows Update Management

- Bugfix: Wird ein Job mit einem `Microsoft Update verwalten` Schritt von `Manuelle Konfiguration` auf `Updateprofil` umgestellt, so werden teilweise noch die vorher vorhandenen Konfigurationen (z.B. Patchfilter) verwendet.

3.6.5 Mobile Devices

- Die von Apple neu eingeführten „Schnellen Sicherheitsmaßnahmen“ werden in der bMC am Endgerät unter `Übersicht – Patch Level`, sowie bei `Geräteinventur` angezeigt. Die Spalte `Patch Level` kann in der Tabellenansicht eingeblendet, sowie in Universellen Dynamischen Gruppen verwendet werden.

- Die Android Enterprise Root-Check Prüfung wurde auf google Play Integrity API umgestellt. Dazu kommuniziert der bServer mit dem baramundi Online Dienst baramundi Root Check Service per https/443.

- Es ist nun möglich, dass der Administrator beim Verteilen eines Exchange-Accounts für iOS-Geräte angibt, welche Services für die Synchronisation aktiv sein sollen. Zusätzlich lässt sich auch einstellen, ob die einzelnen Einstellungen durch den Endbenutzer am Gerät geändert werden können.

- In WLAN-Profilen für Android-Enterprise-Geräte kann die Zufallsgenerierung der MAC-Adresse, analog zu iOS, deaktiviert werden.

- In der bMC kann unter `Konfiguration – Mobile Devices – Android Enterprise` jetzt eine `Standard Play Store App-Verfügbarkeit` eingestellt werden.

- Bugfix: Werden in der bMC unter `Konfiguration - Automatische Registierung - Apple Automated Device Enrollment / DEP` in den Freitextfeldern eines Profils sehr lange Texte eingegeben, so treten Exceptions auf.

- Bugfix: Die Zuweisung von VPP Lizenzen mittels `bMC - Apps – Lizenzen verknüpft` schlägt fehl, wenn viele Benutzer angegeben werden.

- Bugfix: Die Ansicht `bMC – Logische Gruppierung – Inventur – Software (bMD)` ist u.U. sehr verzögert, insbesondere wenn der bMC-Benutzer nicht das Recht hat alle Endgeräte einsehen zu können.

- Bugfix: Werden in einer `Dynamischen Gruppe (Universell)` Mobile-Variablen verwendet, so liefert diese UDG u.U. nach dem Update auf eine baramundi Version 2022 R1 oder 2022 R2 nicht mehr die erwarteten Endgeräte.

3.6.6 bServer

- Es ist möglich im baramundi Datenbankmanager den Kommunikationsmodus mit dem MS-SQL-Server, z.B. TLS mit Zertifikatsvalidierung zu konfigurieren.

- Das Entpacken und Verarbeiten von großen Clientnachrichten, z.B. Inventur und Compliancedaten, wurde verbessert und erfordert jetzt weniger Speicher.

- Bugfix: Das Anlegen einer neuen baramundi Datenbank ist bei Zeitzonen mit UTF+5 nicht möglich und zeigt einen Fehler „*External component has thrown an exception*“

- Bugfix: Der Modern-Management-Microservice startet nicht, wenn eine TLS Verbindung zur Datenbank konfiguriert ist.

3.6.7 bConnect

- bConnect v2 ist jetzt Teil des Produktes.
  bConnect v1.1 kann weiterhin verwendet werden.

- Bugfix: Die Option VLSM lässt sich bei IP-Netzwerken nicht korrekt konfigurieren.

3.6.8 Netzwerkgeräte

- In der bMC kann das Feld `Netzwerkgerät – SNMP – Seriennummer` jetzt auch manuell befüllt werden.

- Bei einem Netzwerk Scan Profil ist die Einstellung `Identifiziere Geräte anhand ihrer IP-Adresse` jetzt Standard.

3.6.9 macOS

- Bugfix: Der "Gerät wiederherstellen" Dialog wird am Gerät angezeigt, obwohl im Enrollment Profil dieser als unterdrückt konfiguriert ist.

- Bugfix: Das Enrollment per SSH ohne Push-Zertifikat funktioniert dann nicht, wenn zuvor ein Enrollment mit Push-Zertifikat durchgeführt wurde.

3.6.10 baraDIP

- Der im baraDIP enthaltene Apache wurde auf 64-Bit Architektur umgestellt. Er kann damit auch nur noch auf 64 Bit Betriebssystemen installiert und betrieben werden.
- Einträge unter `DIP-Verwaltung – DIP-Server – Synchronisation – Includes` unterstützen jetzt auch Angaben mit Wildcard `xxx*`.
- Hinweis: Mit dem kommenden Release 2023 R2 wird für den baraDIP nur noch die sichere Kommunikation per https unterstützt.

3.6.11 bMOL

- bMOL bindet sich automatisch beim ersten Kontakt an das Serverzertifikat. Evtl. vorhandene bMOL-Skripte sind zu prüfen.
- Bitte beachten Sie, dass bMOL eine veraltete Schnittstelle ist. Eine Umstellung auf bConnect wird empfohlen.

4 Anhang

4.1 Glossar

ACPI	Advanced Configuration and Power Interface
AE	Android Enterprise
AMT	Active Management Technologie (Intel vPro)
APN	Access Point Name (Kontext: Mobilfunknetze)
APNS	Apple Push Notification Service
bAPSI	baramundi Push Service Infrastructure
bBT	baramundi Background Transfer
bCenter	baramundi Management Center für iOS (App)
bCM	baramundi Compliance Management
bDS	baramundi Deployment Script
bDX	baramundi Data Exchange
BIOS	Basic Input Output System
Blacklist	Negativliste unerwünschter Apps (siehe baramundi Mobile Devices)
bLM	baramundi License Management
bMA	baramundi Management Agent
bMC	baramundi Management Center
bMD	baramundi Mobile Devices
bMS	baramundi Management Suite
bMS/R	baramundi Management Server/Relay
bMSW	baramundi Managed Software
bND	baramundi Network Devices
bPM	baramundi Patch Management
Client	Synonym für Endpoint
DC	Domain Controller
DEP	Device Enrollment Program (von Apple)
DIP	Distributed Installation Point
Endpoint	Synonym für Client
FDB	Forwarding Database
IEM	Internet-Enabled Endpoint Management (d.h. ohne VPN)
IPv6	Internet Protocol Version 6
JSON	JavaScript Object Notation
GCM	Google Cloud Messaging (Android)

MAM	Mobile Application Management
MCM	Mobile Content Management
MDM	Mobile Device Management
PCI	Peripheral Component Interconnect
PKI	Private Key Infrastructure
REST	Representational State Transfer
SAFE	Samsung For Enterprise (MDM-API)
SAM	Software Asset Management
SCEP	Simple Certificate Enrollment Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TMG	Threat Management Gateway (Microsoft)
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
UI	User Interface (Benutzerschnittstelle)
VM	Virtuelle Maschine
VPN	Virtual Private Network
VPP	Volume Purchase Program (Apple)
Whitelist	Positivliste erlaubter Apps (siehe baramundi Mobile Devices)
WoL	Wake-On-LAN

4.2 Komponenten von Drittherstellern

Informationen zur Lizenzierung von Drittanbietern finden Sie auf dem ISO Image unter:
`..\3rdParty-Licensing\3rdPartyLicenses.pdf`

4.3 Abbildungsverzeichnis